

WIRELESS G
4-PORT
ROUTER
USER
MANUAL
MODEL 524636



INT-524636-UM-0209-02

CONTENTS

1	HARDWARE	6
1.1	Front Panel / LEDs	6
1.2	Rear Panel / Ports & Jacks.....	6
1.3	Connecting the Router.....	7
2	QUICK INSTALLATION.....	8
2.1	Time Zone.....	10
2.2	LAN Settings.....	10
2.3	WAN Interface	11
2.3.1	Static IP	12
2.3.2	DHCP Client	12
2.3.3	PPPoE.....	13
2.3.4	PPTP	13
2.4	Wireless Basic Settings	14
2.5	Wireless Security Settings	15
2.5.1	WEP	16
2.5.2	WPA (TKIP)	17
2.5.3	WPA2 (AES).....	18
2.5.4	WPA2 (Mixed)	18
3	GENERAL SETUP.....	20
3.1	System.....	21
3.1.1	Time Zone Setting.....	21
3.1.2	Password Setup.....	22
3.1.3	Ping Testing	22
3.2	WAN	23
3.2.1	Static IP	24
3.2.2	DHCP Client	25
3.2.3	PPPoE (PPP over Ethernet).....	26
3.2.4	PPTP	27
3.2.5	DDNS	28
3.3	LAN	30
3.4	Wireless.....	32
3.4.1	Basic Settings.....	32
3.4.2	Advanced Settings.....	33
3.4.3	Security	35
3.4.4	Access Control	36
3.5	Firewall	37
3.5.1	URL Filtering	37
3.5.2	Port Filtering.....	38
3.5.3	IP Filtering	39
3.5.4	MAC Filtering.....	40
3.5.5	Port Forwarding.....	41
3.5.6	DMZ.....	42
4	STATUS	43
5	TOOLS	45
	APPENDIX A.....	47
	APPENDIX B	50
	GLOSSARY	51
	SPECIFICATIONS	54

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Wireless G 4-Port Router, Model 524636.

The Wireless G 4-Port Router lets you experience fast speeds as you surf the Web, download music or photos, and play online games. This wireless router works with 802.11g as well as the older 802.11b products, and also includes a four-port 10/100 LAN switch so you can connect using network cable or go wireless to satisfy all your needs.

Keeping intruders out of your network can be a challenge, and this feature-rich wireless router is designed to make that challenge easier. It includes a true firewall that secures your network against hackers. With Network Address Translation (NAT) to shield your networked devices from intruders, plus WEP, WPA and WPA2 encryption to conceal your information on the wireless LAN from eavesdroppers, you can rest assured that you've taken the necessary precautions to protect the data on your network.

The easy-to-follow instructions in this user manual help make setup and operation relatively simple, so you'll soon be enjoying the benefits of these additional features:

- Compatible with all common DSL and cable Internet service providers
- Up to 54 Mbps network data transfer rate
- Supports MAC filtering for wireless clients
- Integrated 10/100 Mbps LAN switch with Auto MDI/MDI-X support
- DHCP server assigns IP addresses for all LAN users
- Supports DDNS (dynamic DNS)
- Supports UPNP (Universal Plug and Play)
- Supports virtual server and DMZ (demilitarized zone)
- VPN Pass Through (PPTP, IPSec, L2TP)
- Integrated anti-DoS firewall
- Content control through IP and Port filters
- Remote management function
- Easy installation through Web-based user interface
- Firmware updates via Web-based user interface
- Lifetime Warranty

NOTE: For a quick install procedure, refer to the printed quick install guide enclosed with this product.

SAFETY & COMPLIANCE STATEMENTS

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of Federal Communications Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment *does* cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to an outlet on a circuit different from the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

This equipment must be installed and operated in accordance with the provided instructions, and a minimum of 20 cm of spacing must be provided between the computer-mounted antenna and a person's body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth

for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation. The antenna(s) used for this transmitter must not be co-located or operated in conjunction with any other antenna or transmitter. The equipment version marketed in the U.S. is restricted to usage of the channels 1-11 only.

R&TTE Compliance Statement

This equipment complies with all the requirements of Directive 1999/5/EC of the European Parliament and the Council of March 9, 1999, on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE directive repeals and replaces Directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines must, therefore, be followed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden and the United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

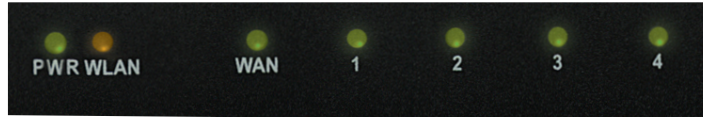
EU Countries Not Intended for Use

None.

1 HARDWARE

1.1 Front Panel / LEDs

The front panel of the Wireless G 4-Port Router features LEDs that provide an immediate indication of the device's operational status.



<u>LED</u>	<u>Status</u>	<u>Description</u>
PWR	On	Power is on.
	Off	Power is off.
WLAN	On	The Wireless LAN has been activated.
	Flashing	There is Wireless LAN activity (transferring or receiving data).
	Off	The Wireless LAN has been deactivated.
WAN	On	The WAN has been connected.
	Flashing	There is WAN activity (transferring or receiving data).
	Off	There is no WAN connection.
1/2/3/4	On	The LAN has been connected.
	Flashing	There is LAN activity (transferring or receiving data).
	Off	There is no LAN connection.

1.2 Rear Panel / Ports & Jacks

The rear panel of the Wireless G 4-Port Router features these ports, buttons and jacks (left to right):



- Four LAN 10/100 Mbps RJ-45 ports for connecting the router to local PCs.
- WAN RJ-45 port for connecting the router to a cable, a DSL modem or the Ethernet.
- Reset button (recessed), which allows you to do two things:
 1. If problems occur with your router, press the button with a pencil tip (for no more than 4 seconds) and the router will re-boot itself, keeping your original configurations.

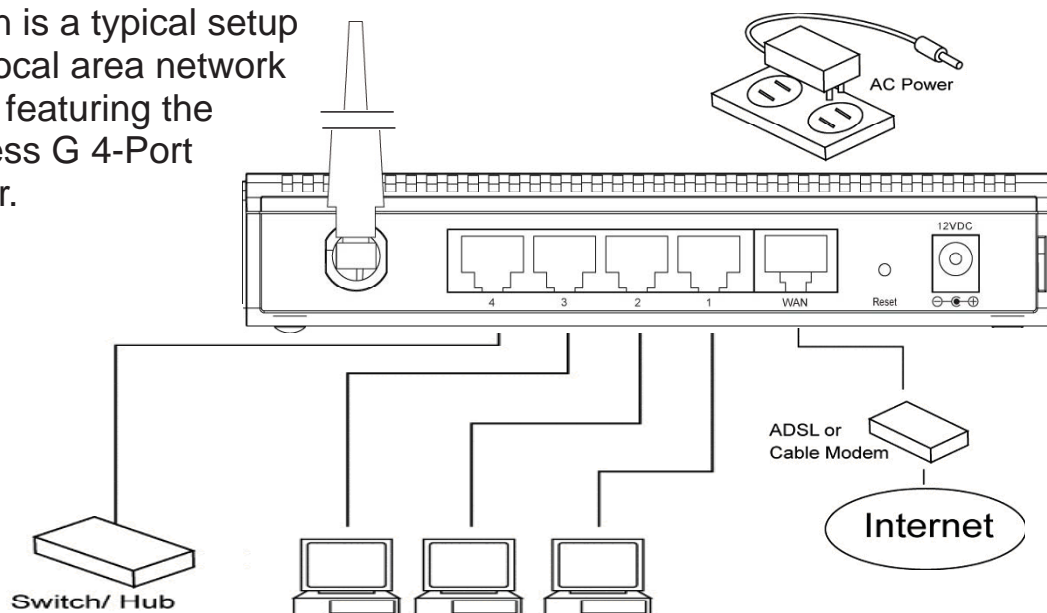
2. If problems persist or you forget your password, press the button for longer than 4 seconds and the router will reset itself to the factory default settings. **NOTE:** Your original configurations will be replaced with the factory default settings.
- Power adapter jack. **NOTE:** Only use the power adapter included with the Wireless G 4-Port Router, as a different adapter could result in product damage.
 - Not shown is the 2 dB dipole antenna, which is connected to the rear panel to the left of the RJ-45 ports.

1.3 Connecting the Router

Before installing the router, connect your PC to the Internet through your broadband service. (If there is any problem, contact your ISP.) Then proceed through the following steps.

1. Turn off your PC(s), cable/DSL modem and the router.
2. Adjust the antenna. Normally, upright is a good place to start.
3. Connect the PC(s) and each switch/hub on your local area network to the LAN ports on the router.
4. Connect the ADSL/DSL/cable modem to the router WAN port.
5. Connect the power adapter between the power socket on the router and an electrical outlet. The router will start to work automatically.
6. Turn on your PC(s) and the cable/(A)DSL modem.

Shown is a typical setup for a local area network (LAN) featuring the Wireless G 4-Port Router.



2 QUICK INSTALLATION

This Quick Installation section can be used to begin router operation as quickly as possible, requiring only minimal information in order to use the router simply as an Internet access device. (A separate printed Quick Install Guide — presenting the basic hardware configuration and the Initial Setup below — is packaged with the Wireless G 4-Port Router.)

First, set up your network; as shown above in Connecting the Router, for example. Then configure your LAN PC clients so they can obtain an IP address automatically. By default, the router's Dynamic Host Configuration Protocol (DHCP) is activated, meaning that once your PCs have been configured to obtain an IP address automatically, all the clients on the network will automatically obtain an IP address, as well. If needed, refer to Appendix A at the back of this manual for the Windows 2000, XP and Vista procedures; for other operating systems, such as Mac and Sun, follow the OS manufacturer's instructions.

Initial Setup

As stated above, once you have configured your PCs to obtain an IP address automatically, the router's DHCP server will automatically give your LAN clients an IP address. To see if you have obtained an IP address, see Appendix B at the back of this manual. **NOTE:** Make sure that this Wireless G 4-Port Router's DHCP server is the only DHCP server available on your LAN. If there is another DHCP on your network, then you'll need to switch one of the DHCP servers off. (To disable the router's DHCP server, refer to Section 3: General Setup / LAN Settings.)

Confirmed that the router has provided an IP address? Then continue with the steps below!

1. Enter the default IP address 192.168.2.1 (the Wireless G 4-Port Router's IP address) into your PC's Web browser and press the Enter key.



2. When the login screen displays, fill in the “User Name” and “Password” fields, then click “OK” to log in. **NOTE:** By default, the user name is “admin” and the password is “1234.” However, for security reasons it is recommended that you change the password as soon as possible (refer to Section 3: General Setup / System / Password Setup).

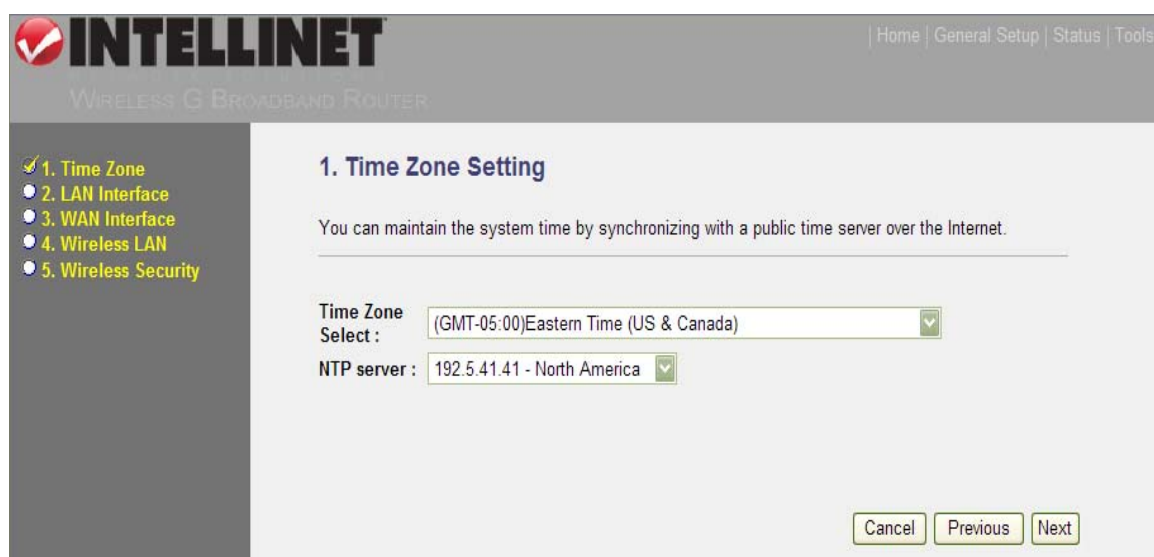
A Windows-style dialog box titled "Connect to 192.168.2.1" with a blue header bar. It features a key icon in the top left. The main area is light beige and contains the text "Default: admin/1234". Below this are two input fields: "User name:" with a dropdown arrow and a small user icon, and "Password:" with a standard text box. A checkbox labeled "Remember my password" is positioned below the password field. At the bottom right are "OK" and "Cancel" buttons.

3. When the Home screen displays (below), click “Quick Setup” to continue with the Quick Installation procedure. The other three main sections shown as menu options on the Home screen — General Setup, Status Information and Tools — are presented and explained in subsequent sections should you wish to use the many additional advanced features of the Wireless G 4-Port Router.

The screenshot shows the Intellinet Wireless G Broadband Router's web interface. At the top is a grey header with the Intellinet logo on the left and navigation links "Home | General Setup | Status | Tools" on the right. Below the header is a dark grey sidebar on the left containing four buttons: "Quick Setup", "General Setup", "Status Info", and "Tools". The main content area on the right is light grey and displays four sections, each with a blue underlined heading and a descriptive paragraph: "Quick Setup Wizard" (describing a wizard for cable or DSL modem configuration), "General Setup" (listing advanced features like DMZ, VPN, and firewall), "Status Information" (describing hardware/firmware status), and "Tools" (describing configuration, firmware upgrade, and reset tools).

2.1 Time Zone

On this screen, you can base the router's time on these settings, which will also affect functions such as log entries and firewall settings.



The screenshot shows the '1. Time Zone Setting' screen of an INTELLINET Wireless G Broadband Router. The left sidebar contains a menu with five items: '1. Time Zone' (selected with a checkmark), '2. LAN Interface', '3. WAN Interface', '4. Wireless LAN', and '5. Wireless Security'. The main content area is titled '1. Time Zone Setting' and includes a sub-header: 'You can maintain the system time by synchronizing with a public time server over the Internet.' Below this, there are two dropdown menus: 'Time Zone Select' with the value '(GMT-05:00)Eastern Time (US & Canada)' and 'NTP server' with the value '192.5.41.41 - North America'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

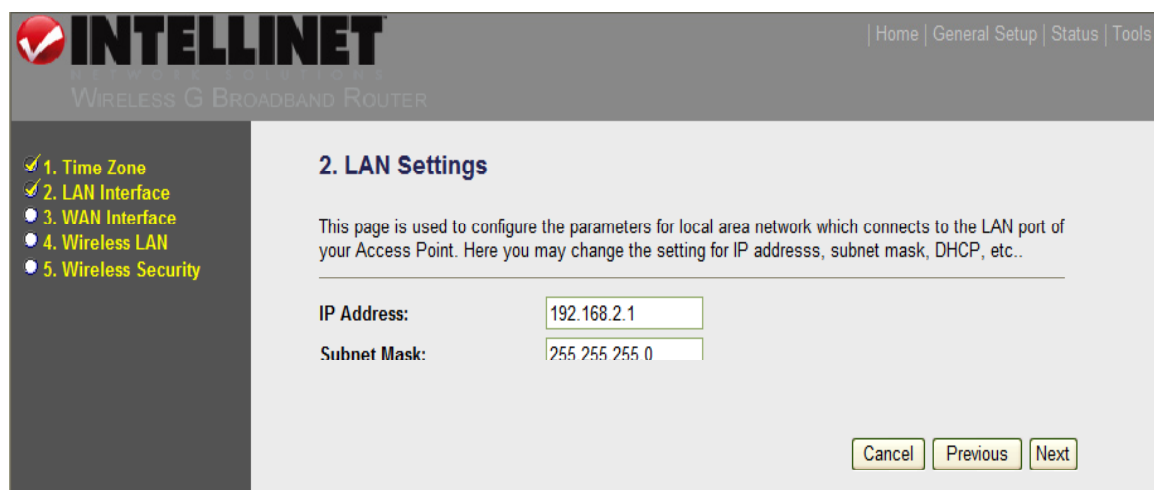
Time Zone Select: Select your local time zone from the drop-down menu. The router will synchronize time according to your selection.

NTP server: Select the time server to synchronize with.

Click "Next" to proceed to the next screen.

2.2 LAN Settings

On this screen, you can configure the parameters for the local area network.



The screenshot shows the '2. LAN Settings' screen of an INTELLINET Wireless G Broadband Router. The left sidebar contains a menu with five items: '1. Time Zone', '2. LAN Interface' (selected with a checkmark), '3. WAN Interface', '4. Wireless LAN', and '5. Wireless Security'. The main content area is titled '2. LAN Settings' and includes a sub-header: 'This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP addresss, subnet mask, DHCP, etc..'. Below this, there are two input fields: 'IP Address' with the value '192.168.2.1' and 'Subnet Mask' with the value '255.255.255.0'. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

IP Address: Enter the router's LAN port IP address (your LAN clients' default gateway IP address).

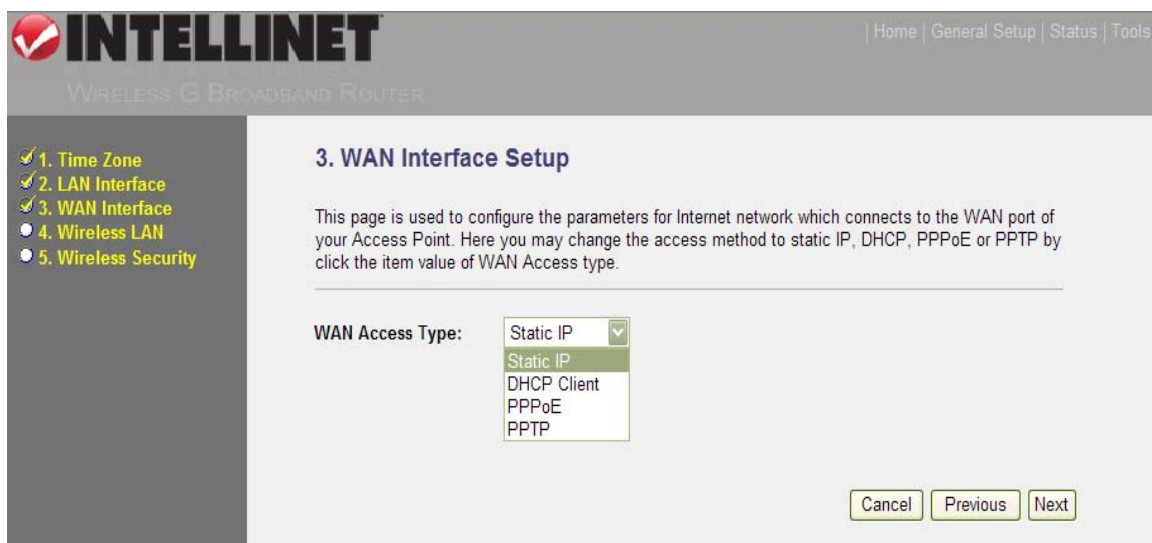
Subnet Mask: Specify a subnet mask for your LAN segment.

Click "Next" to proceed to the next screen.

2.3 WAN Interface

On this screen, select one of the four types of connections you'll be using — Static IP, DHCP Client, PPPoE or PPTP (as explained in the subsections below) — to connect your router's WAN port to your ISP.

NOTE: Different Internet service providers require different Internet connection methods. Check with your ISP as to the type of connection that is required.



WAN Access Type: Select one of the four connection options from the drop-down menu, then click "Next" to proceed to the screen of the selected connection type.

Static IP — Your ISP has given you an IP address already.

DHCP Client — Your ISP will automatically give you an IP address.

PPPoE — Your ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection.

PPTP — Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.

2.3.1 Static IP

The screenshot shows the '3. WAN Interface Setup' page of an INTELLINET router. The left sidebar contains a navigation menu with five items: 1. Time Zone, 2. LAN Interface, 3. WAN Interface (highlighted), 4. Wireless LAN, and 5. Wireless Security. The main content area has a title '3. WAN Interface Setup' and a descriptive paragraph: 'This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.' Below this, there are five input fields: 'WAN Access Type' (a dropdown menu set to 'Static IP'), 'IP Address' (text box with '172.1.1.1'), 'Subnet Mask' (text box with '255.255.255.0'), 'Default Gateway' (text box with '172.1.1.254'), and 'DNS' (empty text box). At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

IP Address: Enter the IP address that your ISP has given you.

Subnet Mask: Enter the ISP-provided subnet mask; e.g., 255.255.255.0.

Default Gateway IP: Enter the ISP's IP address gateway.

DNS: Enter the ISP's DNS server IP address.

Click "Next" to proceed to the next screen.

2.3.2 DHCP Client

The screenshot shows the '3. WAN Interface Setup' page of an INTELLINET router. The left sidebar contains a navigation menu with five items: 1. Time Zone, 2. LAN Interface, 3. WAN Interface (highlighted), 4. Wireless LAN, and 5. Wireless Security. The main content area has a title '3. WAN Interface Setup' and a descriptive paragraph: 'This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.' Below this, there are two input fields: 'WAN Access Type' (a dropdown menu set to 'DHCP Client') and 'Hostname' (empty text box). At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

Hostname: Enter an optional hostname; e.g., "myhome."

Click "Next" to proceed to the next screen.

2.3.3 PPPoE

The screenshot shows the '3. WAN Interface Setup' page of the INTELLINET router's web interface. On the left, a sidebar lists five steps: 1. Time Zone, 2. LAN Interface, 3. WAN Interface (highlighted with a checkmark), 4. Wireless LAN, and 5. Wireless Security. The main content area has a title '3. WAN Interface Setup' and a descriptive paragraph: 'This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.' Below this, there are three input fields: 'WAN Access Type' (a dropdown menu set to 'PPPoE'), 'User Name' (an empty text box), and 'Password' (an empty text box). At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

User Name: Enter the username provided by your ISP.

Password: Enter the password provided by your ISP.

NOTE: Additional parameters, such as idle timeout, MTU size and connection type, can be found in General Setup / LAN Setup.

Click “Next” to proceed to the next screen.

2.3.4 PPTP

The screenshot shows the '3. WAN Interface Setup' page of the INTELLINET router's web interface, similar to the previous one but for PPTP. The sidebar on the left is identical, with '3. WAN Interface' highlighted. The main content area has the same title and descriptive paragraph. Below the paragraph, there are six input fields: 'WAN Access Type' (a dropdown menu set to 'PPTP'), 'IP Address' (a text box containing '0.0.0.0'), 'Subnet Mask' (a text box containing '0.0.0.0'), 'Server IP Address' (an empty text box), 'User Name' (an empty text box), and 'Password' (an empty text box). At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Next'.

IP Address: Enter the IP address your ISP has given you to establish a PPTP connection.

Subnet Mask: Enter the ISP-provided subnet mask; e.g., 255.255.255.0.

Server IP Address: Enter the IP address of the ISP gateway.

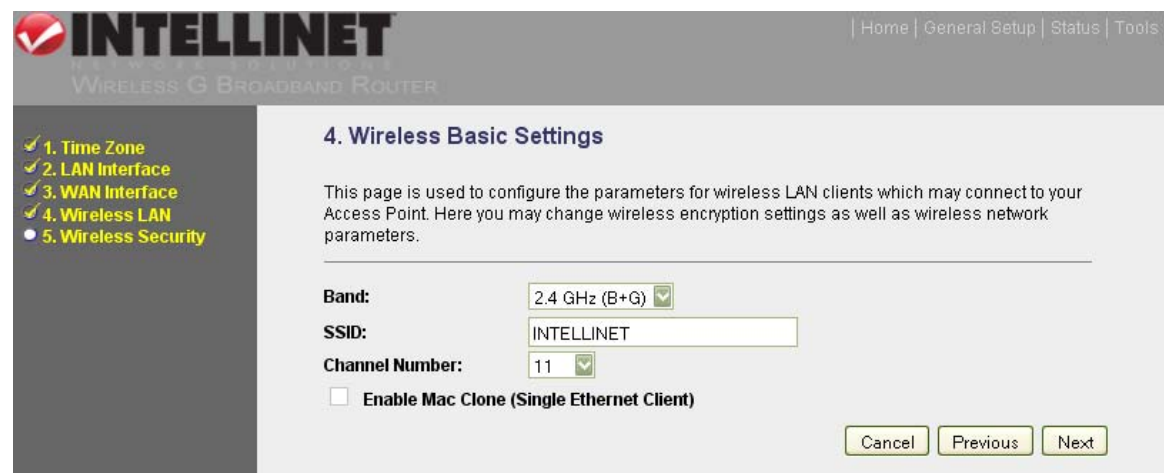
User Name: Enter the username provided by your ISP for the PPTP connection (sometimes referred to as the connection ID).

Password: Enter the password provided by your ISP.

Click “Next” to proceed to the next screen.

2.4 Wireless Basic Settings

This screen displays when you click “Next” after configuring any of the four WAN interfaces above.



Band: This allows you to set the router (acting as an access point) as 802.11b or 802.11g mode. You can also select B+G mode to allow the AP to select either 802.11b or 802.11g automatically.

SSID: Enter a name for the wireless LAN. All the devices in the same wireless LAN should have the same ESSID.

Channel Number: Select the channel to be used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

Enable MAC Clone: Select to allow the router to copy the first seen MAC address to the WLAN MAC.

Click “Next” to proceed to the next screen.

2.5 Wireless Security Settings

Enabling WEP or WPA encryption can prevent unauthorized access to your wireless network.



The screenshot shows the configuration interface for a Wireless G Broadband Router. The top navigation bar includes links for Home, General Setup, Status, and Tools. A sidebar on the left lists five configuration steps: 1. Time Zone, 2. LAN Interface, 3. WAN Interface, 4. Wireless LAN, and 5. Wireless Security (which is highlighted). The main content area is titled '5. Wireless Security' and contains a descriptive paragraph: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' Below this text is an 'Encryption:' label followed by a drop-down menu. The menu is open, showing five options: None, WEP, WPA (TKIP), WPA2(AES), and WPA2 Mixed. At the bottom right of the page are three buttons: 'Cancel', 'Previous', and 'OK'.

Encryption: Select one of the five options from the drop-down menu, then click “OK” to proceed to the screen of the selected option.

None — Do not apply any encryption to wireless usage: Everyone has access without needing permission.

WEP — You can select the WEP key length for encryption: 64-bit or 128-bit. A larger WEP key length will provide a higher level of security, but the throughput will be lower.

WPA (TKIP) — You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. Use TKIP to change the encryption key frequently.

WPA2 (AES) — You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. Use CCMP (AES) to change the encryption key frequently.

WPA2 Mixed — This will automatically select TKIP or AES based on the other communication peer.

2.5.1 WEP

When you select either a 64-bit or 128-bit WEP key, you need to enter WEP keys to encrypt data. You can generate the key by yourself and enter it; you can also enter four WEP keys and select one of them as the default key. Then the router can receive any packets encrypted by one of the four keys.

The screenshot shows the '5. Wireless Security' configuration page of an INTELLINET router. On the left is a sidebar with a list of configuration steps: 1. Time Zone, 2. LAN Interface, 3. WAN Interface, 4. Wireless LAN, and 5. Wireless Security (which is highlighted). The main content area is titled '5. Wireless Security' and contains a description: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' Below this, there are several configuration options: 'Encryption:' with a dropdown menu set to 'WEP'; 'Key Length:' with a dropdown menu set to '64-bit'; 'Key Format:' with a dropdown menu set to 'ASCII (5 characters)'; 'Default Tx Key:' with a dropdown menu set to 'Key 1'; and four text input fields for 'Encryption Key 1:', 'Encryption Key 2:', 'Encryption Key 3:', and 'Encryption Key 4:', each containing five asterisks. At the bottom right of the form are three buttons: 'Cancel', 'Previous', and 'OK'.

Key Length: Select the WEP key length for encryption: 64-bit or 128-bit. A larger WEP key length will provide a higher level of security, but the throughput will be lower.

Key Format: Select ASCII characters (alphanumeric format) or hexadecimal digits (in the “A-F,” “a-f” and “0-9” range) to be the WEP key. For example, ASCII characters: “guest”; hexadecimal digits: “12345abcde.”

Default Tx Key: Select one of the four keys as the default key to encrypt your data.

Encryption Key 1–4: The WEP keys are used to encrypt data transmitted in the wireless network. Fill in the fields using the following guidelines.

- 64-bit WEP: Input 10-digit hex values (in the “A-F,” “a-f” and “0-9” range) or 5-digit ASCII characters as the encryption keys.

- 128-bit WEP: Input 26-digit hex values (in the “A-F,” “a-f” and “0-9” range) or 13-digit ASCII characters as the encryption keys.

Click “OK” to save and activate all the settings. Now you can use the router as your Internet gateway.

2.5.2 WPA (TKIP)

Wi-Fi Protected Access (WPA) is an advanced security standard that lets you use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP to frequently change the encryption key, making it difficult for hackers to break through and thus greatly improving security.



The screenshot shows the configuration interface for the INTELLINET Wireless G Broadband Router. The page title is "5. Wireless Security". A sidebar on the left lists navigation options: 1. Time Zone, 2. LAN Interface, 3. WAN Interface, 4. Wireless LAN, and 5. Wireless Security (which is highlighted). The main content area explains that this page allows setting up wireless security by turning on WEP or WPA using Encryption Keys. It includes three input fields: "Encryption:" with a dropdown menu set to "WPA (TKIP)", "Pre-Shared Key Format:" with a dropdown menu set to "Passphrase", and "Pre-Shared Key:" with a text input field. At the bottom right, there are three buttons: "Cancel", "Previous", and "OK".

Pre-Shared Key Format: Select “Passphrase” (alphanumeric format) or “Hexadecimal Digits” (in the “A-F,” “a-f” and “0-9” range) for the pre-shared key. For example, passphrase: “iamguest”; hex digits: “12345abcde.”

Pre-Shared Key: The pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill in the fields using the following guidelines.

- Hex: Input 64-digit hex values (in the “A-F,” “a-f” and “0-9” range) or at least an 8-character passphrase as the pre-shared keys.

Click “OK” to save and activate all the settings. Now you can use the router as your Internet gateway.

2.5.3 WPA2 (AES)

Wi-Fi Protected Access 2 (WPA2) is an advanced security standard that lets you use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses CCMP (AES) to frequently change the encryption key, making it difficult for hackers to break through and thus greatly improving security.



The screenshot shows the configuration interface for a Wireless G Broadband Router. The top navigation bar includes links for Home, General Setup, Status, and Tools. A sidebar on the left lists five configuration steps: 1. Time Zone, 2. LAN Interface, 3. WAN Interface, 4. Wireless LAN, and 5. Wireless Security (which is highlighted). The main content area is titled '5. Wireless Security' and contains a descriptive paragraph: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' Below this, there are three fields: 'Encryption' with a dropdown menu set to 'WPA2(AES)', 'Pre-Shared Key Format' with a dropdown menu set to 'Passphrase', and 'Pre-Shared Key' with an empty text input field. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'OK'.

Pre-Shared Key Format: Select “Passphrase” (alphanumeric format) or “Hexadecimal Digits” (in the “A-F,” “a-f” and “0-9” range) for the pre-shared key. For example, passphrase: “iamguest”; hex digits: “12345abcde.”

Pre-Shared Key: This is used to authenticate and encrypt data transmitted in the wireless network. Fill in the fields using the following guidelines.

- Hex: Input 64-digit hex values (in the “A-F,” “a-f” and “0-9” range) or at least an 8-character passphrase as the pre-shared keys.

Click “OK” to save and activate all the settings. Now you can use the router as your Internet gateway.

2.5.4 WPA2 Mixed

Wi-Fi Protected Access 2 (WPA2) is an advanced security standard that lets you use a pre-shared key to authenticate wireless stations and encrypt data during communication. This option uses TKIP or CCMP

(AES) to frequently change the encryption key, making it difficult for hackers to break through and thus greatly improving security.

The screenshot shows the configuration interface for an INTELLINET Wireless G Broadband Router. The top navigation bar includes links for Home, General Setup, Status, and Tools. A sidebar on the left lists five configuration steps: 1. Time Zone, 2. LAN Interface, 3. WAN Interface, 4. Wireless LAN, and 5. Wireless Security (which is highlighted). The main content area is titled '5. Wireless Security' and contains a descriptive paragraph: 'This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.' Below this, there are three configuration fields: 'Encryption:' with a dropdown menu set to 'WPA2 Mixed', 'Pre-Shared Key Format:' with a dropdown menu set to 'Passphrase', and 'Pre-Shared Key:' with an empty text input field. At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'OK'.

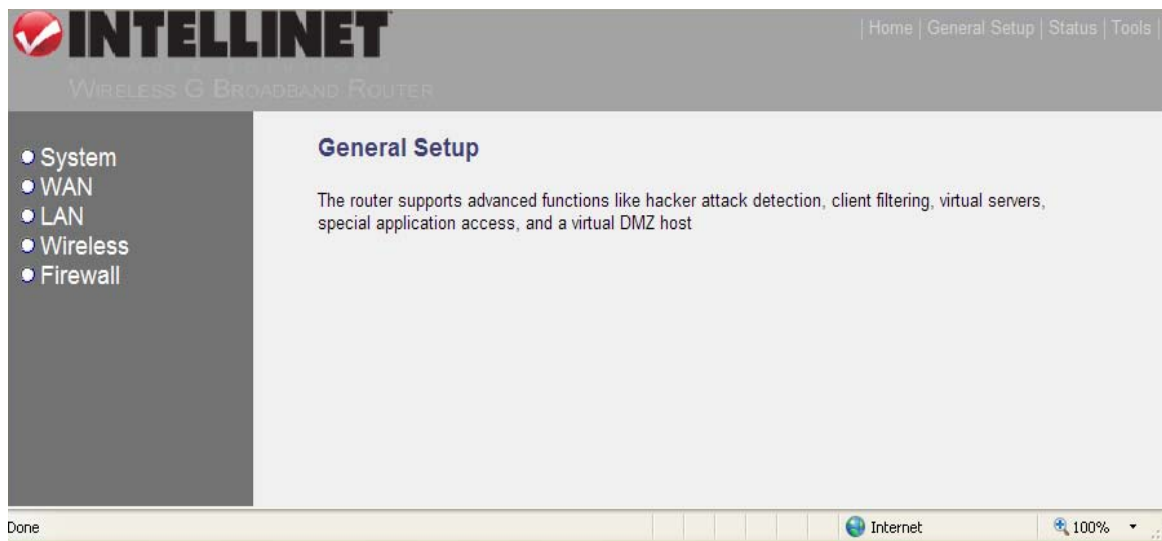
Pre-Shared Key Format: Select “Passphrase” (alphanumeric format) or “Hexadecimal Digits” (in the “A-F,” “a-f” and “0-9” range) for the pre-shared key. For example, passphrase: “iamguest”; hex digits: “12345abcde.”

Pre-Shared Key: This is used to authenticate and encrypt data transmitted in the wireless network. Enter either a 64-digit hex value (in the “A-F,” “a-f” and “0-9” range) or at least an 8-character passphrase.

Click “OK” to save and activate all the settings. Now you can use the router as your Internet gateway.

3 GENERAL SETUP

Clicking “General Setup” on the Home Page — which displays when the initial setup is completed (see Quick Installation) — displays the screen below. If you already configured the Quick Setup Wizard, you *don’t* need to configure anything in the General Setup section in order to start using the Internet. This section *does*, however, allow you to configure the router to meet your network’s more specific needs by using advanced features such as address mapping, access control, hacker-attack prevention and DMZ.



To access the various configuration screens, click/select one of the five subsections listed on the left-hand menu and briefly described below.

System: This section allows you to configure the router’s system time zone and password, and utilize ping testing.

WAN: This section allows you to select the connection method in order to establish a connection with your ISP (as in the Quick Installation section).

LAN: This section allows you to specify the LAN segment’s IP address and subnet mask, enable/disable DHCP and select an IP range for the LAN.

Wireless: This section allows you to set up the wireless LAN’s SSID, WEP key and MAC filtering.

Firewall: This section allows you to configure access control, hacker-attack prevention and DMZ.

3.1 System

Select from among Time Zone Setting, Password Setup and Ping Testing on the left-hand menu to continue with your configuration.

The screenshot shows the 'System Setting' page of the INTELLINET router. The left-hand menu is expanded, showing 'System' as the selected category. Under 'System', there are three sub-items: 'Time Zone Setting' (highlighted in yellow), 'Password Setup', and 'Ping Testing'. Below these are four other categories: 'WAN', 'LAN', 'Wireless', and 'Firewall'. The main content area is titled 'System Setting' and contains a paragraph: 'This page includes all the basic configuration tools for the router. The options are in the menu screen to the left.'

3.1.1 Time Zone Setting

Your router bases its time reference on the settings configured here, which will affect functions such as log entries and firewall settings.

The screenshot shows the 'Time Zone Setting' page of the INTELLINET router. The left-hand menu is expanded, showing 'System' as the selected category. Under 'System', there are three sub-items: 'Time Zone Setting' (highlighted in yellow), 'Password Setup', and 'Ping Testing'. Below these are four other categories: 'WAN', 'LAN', 'Wireless', and 'Firewall'. The main content area is titled 'Time Zone Setting' and contains a paragraph: 'You can maintain the system time by synchronizing with a public time server over the Internet.' Below this paragraph are several form fields: 'Current Time' (Yr: 2009, Mon: 1, Day: 21, Hr: 9, Min: 12, Sec: 49), 'Time Zone Select' (a dropdown menu showing '(GMT-05:00)Eastern Time (US & Canada)'), 'Enable NTP client update' (a checked checkbox), 'NTP server' (a dropdown menu showing '192.5.41.41 - North America'), and a 'Manual IP Setting' option (a radio button and an empty text box). At the bottom right are three buttons: 'Apply', 'Cancel', and 'Refresh'.

Current Time: Set the current time.

Time Zone Select: The router will set its time based on this selection.

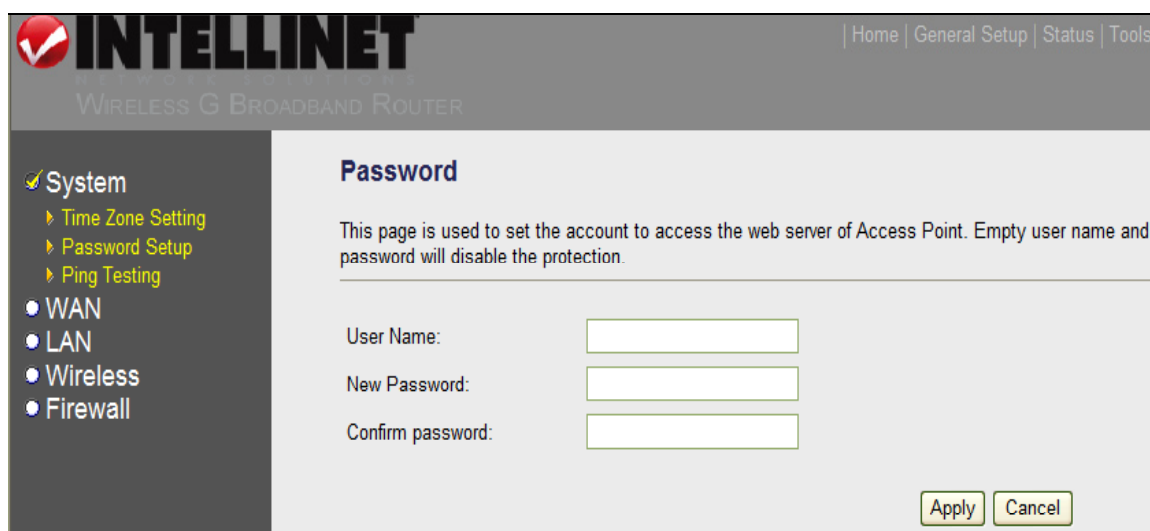
Enable NTP client update: Check the box to enable the router to update the time from the NTP server.

NTP server: Select a preset time server or manually input a server IP.

Click "Apply" to save the configurations.

3.1.2 Password Setup

You can change the password required to log in to the router system's Web-based management. By default, there is no password, so assign a password to the administrator as soon as possible and record it in a safe place. Passwords can contain up to 12 alphanumeric characters and are case sensitive.



The screenshot shows the Intellinet Web-based management interface. The top header includes the Intellinet logo and navigation links: Home | General Setup | Status | Tools. Below the header, the page is titled "PASSWORD SETUP" and "WIRELESS G BROADBAND ROUTER". On the left, a sidebar menu shows "System" as the active section, with sub-items: Time Zone Setting, Password Setup (highlighted), and Ping Testing. Below these are links for WAN, LAN, Wireless, and Firewall. The main content area is titled "Password" and contains a descriptive text: "This page is used to set the account to access the web server of Access Point. Empty user name and password will disable the protection." Below this text are three input fields labeled "User Name:", "New Password:", and "Confirm password:". At the bottom right of the form are "Apply" and "Cancel" buttons.

User Name: Change your login username in this field.

New Password: Enter your new password in this field.


Confirmed Password: Enter your new password again for verification.

NOTE: If you forget your password, you'll have to reset the router to the factory default (no password) with the reset button (see Hardware).

Click "Apply" to save the configurations.

3.1.3 Ping Testing

With this tool you can test your Internet connection as well as the status of a certain host. The example below shows the test results for the domain "intellinet-network.com."


INTELLINET
NETWORK SOLUTIONS
 WIRELESS G BROADBAND ROUTER

[Home](#) | [General Setup](#) | [Status](#) | [Tools](#)

- System
 - Time Zone Setting
 - Password Setup
 - Ping Testing
- WAN
- LAN
- Wireless
- Firewall

Ping Testing

This is a handy tool for user to test LAN or WAN connectivity by invoking ping command.

IP Address / Host Name


Response

```

PING intellinet-network.com (72.15.195.103): 56 data bytes
64 bytes from 72.15.195.103: icmp_seq=0 ttl=54 time=90.0 ms
64 bytes from 72.15.195.103: icmp_seq=1 ttl=54 time=80.0 ms
64 bytes from 72.15.195.103: icmp_seq=2 ttl=54 time=80.0 ms
64 bytes from 72.15.195.103: icmp_seq=3 ttl=54 time=80.0 ms

--- intellinet-network.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 80.0/82.5/90.0 ms
        
```

If the host or IP address you try to ping is offline or otherwise unavailable, the response will be “Destination Unreachable,” as shown below.


INTELLINET
NETWORK SOLUTIONS
 WIRELESS G BROADBAND ROUTER

[Home](#) | [General Setup](#) | [Status](#) | [Tools](#)

- System
 - Time Zone Setting
 - Password Setup
 - Ping Testing
- WAN
- LAN
- Wireless
- Firewall

Ping Testing

This is a handy tool for user to test LAN or WAN connectivity by invoking ping command.

IP Address / Host Name

Response Destination Unreachable

3.2 WAN

Go to WAN Interface Setup if you’ve already done the Quick Installation setup and want to change your Internet connection to one of the four access types below.

- System
- WAN
 - WAN Interface Setup
 - DDNS
- LAN
- Wireless
- Firewall

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type:

Static IP: Your ISP has given you an IP address already.

DHCP Client: Your ISP will automatically give you an IP address.

PPPoE: Your ISP requires a PPPoE connection.

PPTP: Your ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection.

3.2.1 Static IP

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: Static IP

IP Address: 172.1.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 172.1.1.254

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address: 000000000000 Clone MAC Address

☒ Enable uPNP

☐ Enable Web Server Access on WAN Port: 80

☒ Enable FTP ALG on Port: 21

☒ Enable IPsec pass through on VPN connection

☒ Enable PPTP pass through on VPN connection

☒ Enable L2TP pass through on VPN connection

Apply Cancel

IP Address: Enter the IP address that your ISP has given you.

Subnet Mask: Enter the IP-provided subnet mask (e.g., 255.255.255.0).

Default Gateway: Enter the IP address of ISP's gateway.

DNS 1: Enter the IP address of the DNS server provided by your ISP.

DNS 2/3: Enter IP addresses of other DNS servers provided by your ISP.

Clone MAC Address: Enter the MAC address of your computer if your service provider only permits computers with certain MAC addresses to access the Internet.

Enable UPnP: By enabling this feature, all client systems that support Universal Plug and Play can discover this router automatically and access the Internet through this router without any configuration. The NAT Traversal function provided by UPnP can let applications

that support UPnP smoothly connect to Internet sites without any incompatibility problem due to the NAT port translation.

Enable Web Server Access on WAN Port: Enter where to start the Web server access on the WAN when you want to access the Web-based management from a remote site.

Enable FTP ALG on Port: The FTP Application Layer Gateway is used to manage the File Transfer Protocol (FTP). FTP uses two communication channels: one for control commands and one for the actual files being transferred. When an FTP session is opened, the FTP client establishes a TCP connection (the control channel), usually to Port 21 on the FTP server. You can specify the port here.

Enable IPsec/PPTP/L2TP pass through on VPN connection: Check to select these options if you need to create VPN connections to a remote location, such as your office. If you're not sure which of the protocols you need, you may activate all three.

Click "Apply" to save the configurations.

3.2.2 DHCP Client

This is similar to the DHCP Client screen in Quick Installation, but some ISPs may require additional information beyond the hostname.

System
✓ **WAN**
 ▶ WAN Interface Setup
 ▶ DDNS
• LAN
• Wireless
• Firewall

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

WAN Access Type: DHCP Client

Hostname:

☒ Obtain DNS Automatically
☐ Set DNS Manually

DNS 1:
DNS 2:
DNS 3:

Clone MAC Address: Clone MAC Address

☒ Enable uPNP
☐ Enable Web Server Access on WAN Port:
☒ Enable FTP ALG on Port:
☒ Enable IPsec pass through on VPN connection
☒ Enable PPTP pass through on VPN connection
☒ Enable L2TP pass through on VPN connection

Apply Cancel

Host Name: Enter the hostname of your computer. **NOTE:** This is optional, required only if your service provider asks you to do so.

Obtain DNS Automatically: Select if your ISP requires you to obtain a DNS via the DHCP server before you connect to the Internet.

Set DNS Manually: Select if your ISP gives you a static DNS server for connecting to the Internet.

DNS 1: Enter the IP address of the DNS server provided by your ISP.

DNS 2/3: Enter IP addresses of other DNS servers provided by your ISP.

Clone MAC Address: Enter the MAC address of your computer if your service provider only permits computers with certain MAC addresses to access the Internet.

NOTE: The remaining features/options are identical to those in the Static IP section above.

Click “Apply” to save the configurations.

3.2.3 PPPoE (PPP over Ethernet)

The screenshot shows a web interface for configuring the WAN interface. On the left is a sidebar menu with options: System, WAN (selected), DDNS, LAN, Wireless, and Firewall. The main area is titled 'WAN Interface Setup'. It contains a description: 'This page is used to configure the parameters for Internet network which connects to the WAN port of your router. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by clicking the corresponding item.' Below this, the 'WAN Access Type' is set to 'PPPoE'. Fields for 'User Name', 'Password', and 'Service Name' are provided. 'Connection Type' is set to 'Continuous', with 'Connect' and 'Disconnect' buttons. 'Idle Time' is set to 5 minutes, and 'MTU Size' is set to 1412 bytes. There are radio buttons for 'Obtain DNS Automatically' and 'Set DNS Manually' (selected). Below these are fields for 'DNS 1', 'DNS 2', and 'DNS 3'. A 'Clone MAC Address' field is set to '000000000000'. There are checkboxes for 'Enable uPNP' and 'Enable Web Server Access on WAN'. At the bottom are 'Apply' and 'Cancel' buttons.

User Name: Enter the username assigned by your ISP.

Password: Enter the password assigned by your ISP.

Service Name: Enter a name for this Internet service (optional).

Connection Type: Select one of three Internet connection types:

- Continuous — Keeps an Internet connection alive (no disconnect).
- Connect on Demand — Only connects to the Internet when a connect attempt is made.

- Manual — Only connects to the Internet when “Connect” is clicked; disconnects when “Disconnect” is clicked.

Idle Time: Specify the amount of Internet-inactivity time that needs to elapse before shutting down. **NOTE:** This option is only available when “Connect on Demand” is selected.

MTU Size: Enter the MTU value of your network connection. If unknown, you can use the default value.

Obtain DNS Automatically: Select if your ISP requires you to obtain a DNS via the DHCP server before you connect to the Internet.

Set DNS Manually: Select if your ISP gives you a static DNS server for connecting to the Internet.

DNS 1: Enter the IP address of the DNS server provided by your ISP.

DNS 2/3: Enter IP addresses of other DNS servers provided by your ISP.

Clone MAC Address: Enter the MAC address of your computer if your service provider only permits computers with certain MAC addresses to access the Internet.

NOTE: The remaining features/options are identical to those in the Static IP section above.

Click “Apply” to save the configurations.

3.2.4 PPTP

- System
- WAN
 - WAN Interface Setup
 - DDNS
- LAN
- Wireless
- Firewall

WAN Interface Setup

This page is used to configure the parameters for Internet network which connects to the WAN port of your router. Here you may change the access method to static IP, DHCP, PPPoE or PPTP by clicking the corresponding item .

WAN Access Type: PPTP

IP Address:

Subnet Mask:

Server IP Address:

User Name:

Password:

MTU Size: (1400-1492 bytes)

☐ Obtain DNS Automatically

☒ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Clone MAC Address:

IP Address: Enter the IP address that your ISP has given you.

Subnet Mask: Enter the IP-provided subnet mask (e.g., 255.255.255.0).

Server IP Address: Enter the IP address of the PPTP gateway assigned by your ISP.

User Name: Enter the username assigned by your ISP.

Password: Enter the password assigned by your ISP.

MTU Size: Enter the MTU value of your network connection. If unknown, you can use the default value.

Obtain DNS Automatically: Select if your ISP requires you to obtain a DNS via the DHCP server before you connect to the Internet.

Set DNS Manually: Select if your ISP gives you a static DNS server for connecting to the Internet.

DNS 1: Enter the IP address of the DNS server provided by your ISP.

DNS 2/3: Enter IP addresses of other DNS servers provided by your ISP.

Clone MAC Address: Enter the MAC address of your computer if your service provider only permits computers with certain MAC addresses to access the Internet.

NOTE: The remaining features/options are identical to those in the Static IP section above.

Click “Apply” to save the configurations.

3.2.5 DDNS

DDNS (Dynamic Domain Name System) allows you to map the static domain name to a dynamic IP address. You need to obtain an account, password and your static domain name from the DDNS service provider. This Wireless G 4-Port Router supports DynDNS.org and TZO.

Enable DDNS: Check/select to enable/disable the router’s DDNS function. **NOTE:** The default setting is “Disabled.”


Service Provider: Select a DDNS service provider.

Domain Name: Enter your static domain name for use with DDNS.

User Name/Email: Enter the account identification your DDNS service provider assigned to you.

Password/Key: Enter the password you set for the DDNS service account above.

Click “Apply” to save the configurations.


INTELLINET
NETWORK SOLUTIONS

[Home](#) | [General Setup](#) | [Status](#) | [Tools](#)

WIRELESS G BROADBAND ROUTER

- System
- ✓ WAN
 - ▶ WAN Interface Setup
 - ▶ DDNS
- LAN
- Wireless
- Firewall

DDNS

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☐ **Enable DDNS**

Service Provider : DynDNS

Domain Name :

User Name/Email:

Password/Key:

Status: DDNS is disabled

Note:
For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)!
For DynDNS, you can create your DynDNS account. [here](#)

Apply Cancel

How to Use dyndns.org


DynDNS.com
by Dynamic Network Services Inc.

→

User: Pass: Login

[Lost Password?](#) - [Create Account](#)

[About](#) | [Services](#) | [Account](#) | [Support](#) | [News](#)

The same username and password required to log in to the dyndns.org Web site to manage your accounts (above) need to be entered for the DDNS configuration of the router (below).

DDNS

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☒ **Enable DDNS**

Service Provider : DynDNS

Domain Name :

User Name/Email:

Password/Key: ←

Status: DDNS is disabled

Note:
For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)!
For DynDNS, you can create your DynDNS account. [here](#)

Apply Cancel

Host Services		
Hostname myintellinetrouter.dyndns.org created.		
Hostname	Service	Details
myintellinetrouter.dyndns.org	Host	  

Check that the hostname in your dyndns.org account (above) is the same as the hostname entered into the router's DDNS configuration (below). If it is, click "Apply" to save the settings.

DDNS

Dynamic DNS is a service, that provides you with a valid, unchanging, internet domain name (an URL) to go with that (possibly everchanging) IP-address.

☒ **Enable DDNS**

Service Provider : DynDNS

Domain Name : intellinetrouter.dyndns.org

User Name/Email: username

Password/Key: *****


Status: DDNS is disabled

Note:
For TZO, you can have a 30 days free trial [here](#) or manage your TZO account in [control panel](#)
For DynDNS, you can create your DynDNS account. [here](#)

Apply Cancel

3.3 LAN

This screen allows you to specify a private IP address for your router's LAN ports, as well as a subnet mask for your LAN segment.


Home | General Setup | Status | Tools

WIRELESS G BROADBAND ROUTER

- System
- WAN
- LAN**
- Wireless
- Firewall

LAN Settings

This page is used to configure the parameters for local area network which connects to the LAN port of your Access Point. Here you may change the setting for IP address, subnet mask, DHCP, etc..

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DHCP: Server

DHCP Client Range: 192.168.2.100 - 192.168.2.200 Show Client

802.1d Spanning Tree: Disabled

Clone MAC Address: 000000000000

Apply Cancel

IP Address: This is the router's LAN port IP address (your LAN clients' default gateway IP address). The default is 192.168.2.1.

Subnet Mask: Specify a subnet mask for your LAN segment. The default is 255.255.255.0.

Default Gateway: Specify the default gateway for your LAN segment.

DHCP: Select the DHCP type for your LAN segment.

- **Server** — This is the default setting. The router will automatically give your LAN clients an IP address.
- **Client** — The router will get an IP address from the LAN DHCP server automatically. If the DHCP server is not enabled, you'll need to manually set your LAN clients' IP addresses. If you want the router to be your LAN client's default gateway, make sure that LAN Client is in the same subnet as this router.

DHCP Client Range: Enter an IP address range for your DHCP server to issue IP addresses to your LAN clients. **NOTE:** By default, this IP range is from 192.168.2.100 to 192.168.2.199. If you want your PC to have a static/fixed IP address, you'll need to choose an IP address outside this IP address pool, or range.

Show Client: Click to display a list of connected computers that have obtained an IP address from the router's DHCP server. **NOTE:** Computers with a static IP address setup aren't shown. Click "Refresh" on this sub-screen to update the information.

DHCP		
This table shows the assigned IP address, MAC address and time expired for each DHCP leased client.		
IP Address	MAC Address	Time Expired(s);
192.168.2.105	00:18:8b:b8:8f:f3	857945
Refresh	Close	

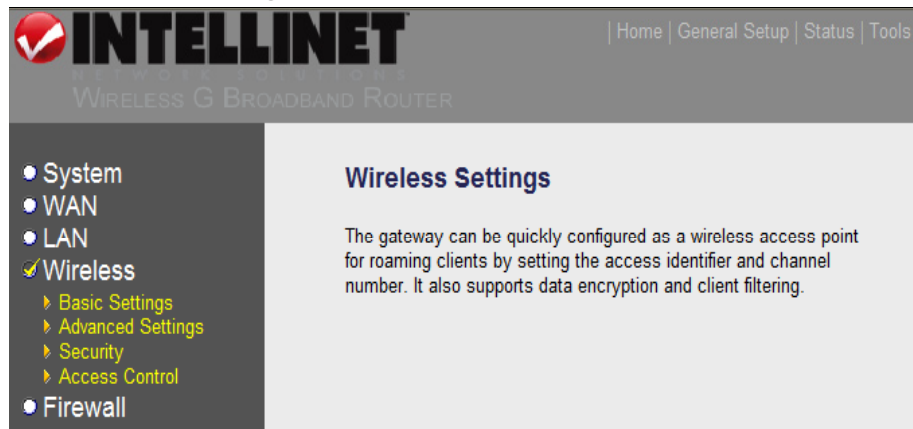
802.1d Spanning Tree: If this function is enabled, this router will use the Spanning Tree protocol to prevent a network loop from occurring in the LAN ports. The default is "Disabled."

Clone MAC Address: Specify the MAC address for your LAN interface. Click "Apply" to save the configurations.

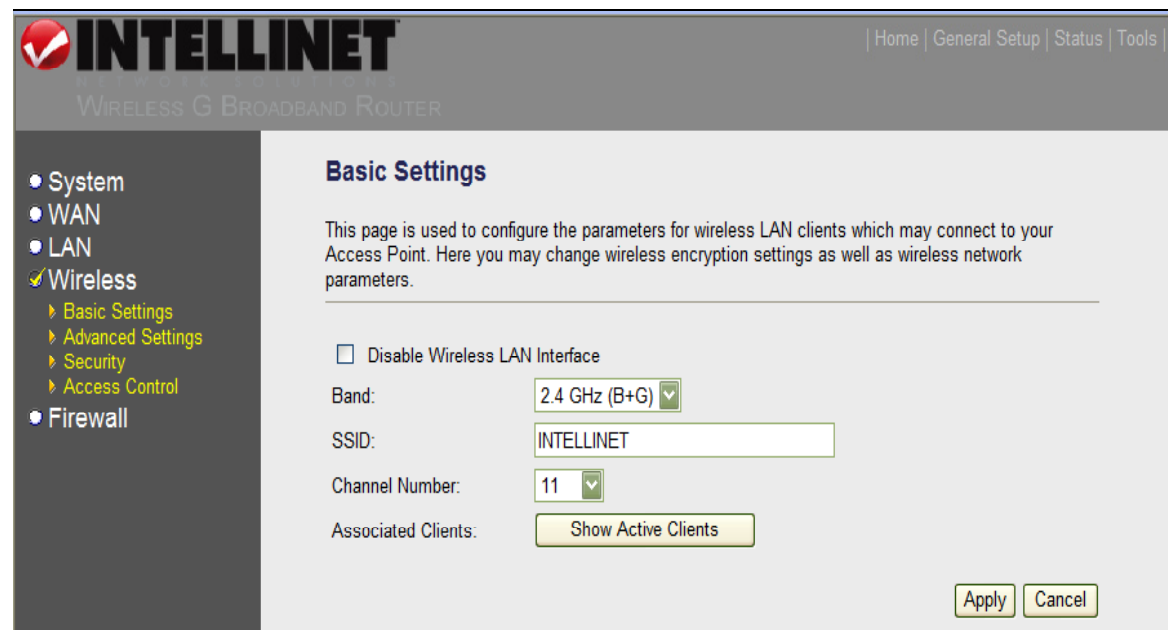
3.4 Wireless

This section allows you to build a wireless LAN so that all PCs equipped with an IEEE 802.11b or 801.11g wireless network adapter can connect to your intranet.

It supports WEP, WPA and WPA2 encryption to enhance the security of your wireless network.



3.4.1 Basic Settings



Disable Wireless LAN Interface: Check/select this box to disable the wireless function.

Band: Select “802.11b” or “802.11g.” You also can select the B+G mode to allow the router to select either the 802.11b or 802.11g connection automatically.

SSID: Enter the name of the wireless LAN. All devices in the same

wireless LAN should have the same ESSID. The default entry is “INTELLINET.”

Channel Number: Select a wireless LAN channel. All devices in the same wireless LAN should use the same channel. The default is 11.

Associated Clients: Click “Show Active Clients” to display the Active Wireless Client table, which shows the status of all active wireless stations that are connecting to the router (as an access point).

Click “Apply” to save the configurations.

3.4.2 Advanced Settings

You can set advanced wireless LAN parameters in this section; however, changes aren’t recommended unless you know what effect the changes will have on this router.

The screenshot shows the 'Advanced Settings' page for an INTELLINET Wireless G Broadband Router. The left sidebar contains a navigation menu with 'System', 'WAN', 'LAN', 'Wireless' (selected), and 'Firewall'. Under 'Wireless', there are sub-links for 'Basic Settings', 'Advanced Settings' (highlighted), 'Security', and 'Access Control'. The main content area is titled 'Advanced Settings' and includes a warning: 'These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.' The settings are as follows:

Setting	Value	Range/Options
Authentication Type:	<input checked="" type="radio"/> Open System <input type="radio"/> Shared Key <input checked="" type="radio"/> Auto	
Fragment Threshold:	2346	(256-2346)
RTS Threshold:	2347	(0-2347)
Beacon Interval:	100	(20-1024 ms)
Data Rate:	Auto	
Preamble Type:	<input checked="" type="radio"/> Long Preamble <input type="radio"/> Short Preamble	
Broadcast SSID:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
IAPP:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
802.11g Protection:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
WMM:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
RF Output Power:	<input checked="" type="radio"/> 100% <input type="radio"/> 50% <input type="radio"/> 25% <input type="radio"/> 10% <input type="radio"/> 5%	
Turbo Mode:	<input checked="" type="radio"/> Auto <input type="radio"/> Always <input type="radio"/> Off	

Note: "Always" may have compatibility issue. "Auto" will only work with Realtek product.

Buttons: Apply, Cancel

Authentication Type: There are three authentication options:

- Open System — This allows wireless stations to associate with the router without WEP encryption.

- **Shared Key** — With this option, you should also set up the WEP key on the Encryption screen, and wireless stations should use WEP encryption in the authentication phase to associate with the router.
- **Auto** — This allows wireless clients to associate with the router by using either of the two authentication types.

Fragment Threshold: Enter the maximum packet size during the fragmentation of data to be transmitted. **NOTE:** If you set this value too low, it will result in poor performance.

RTS Threshold: When the packet size is smaller than the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval: Enter a time interval for the router's beacon broadcast. The beacon is used to synchronize the wireless network.

Data Rate: This is the rate the router (as an access point) transmits data packets. The AP will use the highest possible selected rate.

Preamble Type: "Long Preamble" can provide better wireless LAN compatibility; "Short Preamble" can provide better performance.

Broadcast SSID: When this function is enabled, every wireless station located within range can discover this access point. (If you're building a public wireless network, enabling this feature is recommended.) Disabling, however, can provide better security.

IAPP: Enabling this function allows wireless stations to roam between IAPP-enabled access points within the same wireless LAN.

802.11g Protection: Enabling this function (also called CTS Protection) is recommended to activate the protection mechanism, which can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the AP's throughput will be a bit lower due to more transmitted frame traffic.

WMM: Enabling Wi-Fi MultiMedia (which is recommended) will enhance the data transfer performance of multimedia content when it's being transferred over the wireless network.

RF Output Power: You'll want to use maximum power (100%) most of the time, but there may be instances when the distance between the wireless client and the router is very short and a lower power output is enough to create a fast and stable connection. In those instances, reducing the power output can help keep unauthorized users from breaking in to your wireless network.

Turbo Mode: This enhances the data transfer rate of a WLAN (up to 35 Mbps). The default setting, “Auto,” is recommended.

Click “Apply” to save the configurations.

3.4.3 Security

As an access point, the Wireless G 4-Port Router provides complete wireless LAN security functions — WEP, IEEE 802.11x, IEEE 802.11x with WEP, WPA with pre-shared key and WPA with RADIUS — which protect your wireless LAN from illegal access. Make sure your wireless stations enable the same security function.

The screenshot shows the 'Security' configuration page of an INTELLINET Wireless G Broadband Router. The page has a sidebar on the left with navigation links: System, WAN, LAN, Wireless (selected), Basic Settings, Advanced Settings, Security, Access Control, and Firewall. The main content area is titled 'Security' and contains the following fields and options:

- Encryption:** A dropdown menu currently set to 'None'. To its right is a 'Set WEP Key' button.
- ☐ Use 802.1x Authentication
- WPA Authentication Mode:** Radio buttons for Enterprise (RADIUS) and Personal (Pre-Shared Key) (selected).
- WPA Cipher Suite:** Radio buttons for TKIP and AES (selected).
- WPA2 Cipher Suite:** Radio buttons for TKIP and AES (selected).
- Pre-Shared Key Format:** A dropdown menu set to 'Passphrase'.
- Pre-Shared Key:** A text input field.
- ☐ Enable Pre-Authentication
- Authentication RADIUS Server:** Fields for Port (1812), IP Address, and Password.

A note at the bottom states: "Note: When encryption WEP is selected, you must set WEP key value." At the bottom right are 'Apply' and 'Cancel' buttons.

Encryption: Mode options are “None,” “WEP,” “WPA,” “WPA2” and “WPA2 mixed.” If WEP encryption is selected in the drop-down menu, click “Set WEP Key” and select either “WEP 64 bits” (which is the default setting) or “WEP 128 bits.” The larger key length provides a higher level of security, but the throughput will be lower.

Use 802.1x Authentication: IEEE 802.1x is an authentication protocol. Every user must use a valid account to log in to this access point

before accessing the WLAN. Authentication is processed by a RADIUS server. Check this box to authenticate users by IEEE 802.1x.

WPA Authentication Mode: WPA can authenticate by enabling either “RADIUS” or “Pre-Shared Key.”

WPA / WPA2 Cipher Suite: Select either “TKIP” or “AES” as the WPA / WPA2 key exchange method.

Pre-Shared Key Format: Select “Passphrase” (alphanumeric format) or “Hexadecimal Digits” (in the “A-F,” “a-f” and “0-9” range) for the pre-shared key. For example, passphrase: “iamguest”; hex digits: “12345abcde.”

Pre-Shared Key: This is used to authenticate and encrypt data transmitted in the wireless network. Enter either a 64-digit hex value (in the “A-F,” “a-f” and “0-9” range) or at least an 8-character passphrase.

Authentication Radius Server: Fill in the fields for the port, IP address and password to be used for the external RADIUS server.

Click “Apply” to save the configurations.

3.4.4 Access Control

This screen allows you to control MAC addresses to prevent unauthorized access to your wireless network.

INTELLINET WIRELESS G BROADBAND ROUTER

Home | General Setup | Status | Tools

- System
- WAN
- LAN
- ✓ Wireless
 - ▶ Basic Settings
 - ▶ Advanced Settings
 - ▶ Security
 - ▶ Access Control
- Firewall

Access Control

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

Wireless Access Control Mode:

MAC Address: Comment:

Comment:

MAC Address	Comment	Select
-------------	---------	--------

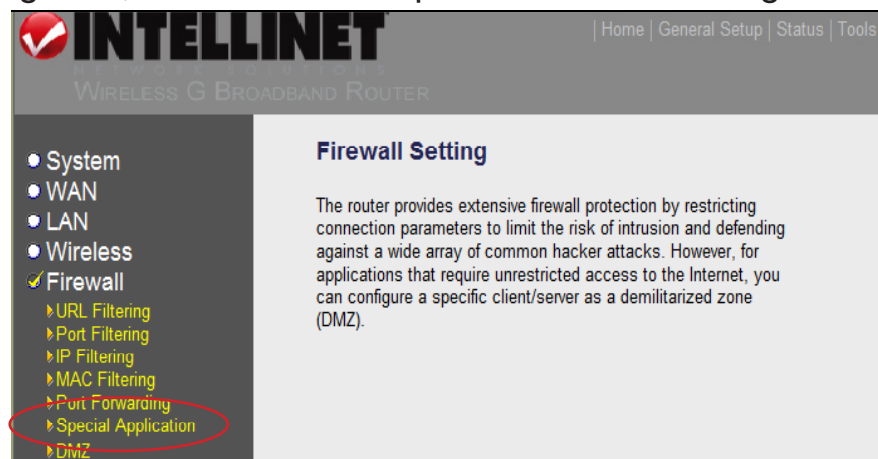
Wireless Access Control Mode: Enable or disable this function.

MAC Address / Comment: Fill in these two fields for the wireless station to be added to the access list, then click “Apply.” Once one or more MAC addresses are given access to the network, the resulting list will display at the bottom of the screen. To remove an address from the list (thus denying access), highlight it and click “Delete Selected” (or “Delete All” if you’ve highlighted more than one). To clear all of your current selections, click “Reset.”

3.5 Firewall

The Wireless G 4-Port Router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of a hacker attack and defending against a wide array of common Internet attacks.

NOTE: Some programs, such as Internet phones and network games or file-sharing programs, need more than one connection, but because of the firewall may not work correctly unless you go to the Special Applications subsection and



follow the steps that make those programs compatible with the router.

3.5.1 URL Filtering

With URL filtering, you can block access to any Web site or Web page that contains a blacklisted keyword, ideal for limiting children’s exposure to unsuitable Web content.

Enable URL Filtering: Select to activate the function.

URL Address: Enter the keyword or part of the URL in the text field, then click “Apply” to add the keyword to the setup.

Once one or more items are listed, the resulting Current Filter Table list can be displayed. Delete individual listings in the URL Address column by checking the corresponding box in the Select column and then clicking “Delete Selected.” Delete all items on the list at once by clicking “Delete All.” To clear all of your current selections, click “Reset.”

Current Filter Table:	
URL Address	Select
www.intellinet-network.com	<input type="checkbox"/>
intellinet-network.com	<input type="checkbox"/>
network	<input type="checkbox"/>
ads	<input type="checkbox"/>

Examples of Filters and Effects

www.intellinet-network.com: Access to the Web site www.intellinet-network.com will be blocked, but access to intellinet-network.com is still allowed (note the missing “www”).

intellinet-network.com: Access to both www.intellinet-network.com and intellinet-network.com is blocked.

network: Access is blocked to any Web site that contains the keyword “network,” such as intellinet-network.com, networkipcamera.com or networksolutions.com. Furthermore, this prevents you from searching for the keyword “network” using a search engine; e.g., Google.


ads: This filter can help reduce the amount of advertisements shown on Web pages. It will prevent any content that resides in a location (www.domain.com/images/ads/, as an example) from loading.

3.5.2 Port Filtering

This section allows you to prevent users from accessing certain Internet applications/services (e.g., Web sites, e-mail, FTP sites) by restricting the flow of certain types of data packets. (Also see IP Filtering below.)

Enable Port Filtering: Select to activate the function.

Port Range / Protocol / Comment: For any item you want to include in your port-filtering efforts, enter a port range, select one of the protocols from the drop-down menu, add any comments that can help identify the item whenever you refer to the list, then click “Apply.” Once one or more items are listed, the resulting Current Filter Table list will display at the bottom of the screen. To remove an item from


INTELLINET
WIRELESS G BROADBAND ROUTER

[Home](#) | [General Setup](#) | [Status](#) | [Tools](#)

- System
- WAN
- LAN
- Wireless
- Firewall**
 - URL Filtering
 - Port Filtering
 - IP Filtering
 - MAC Filtering
 - Port Forwarding
 - Special Application
 - DMZ

Port Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable Port Filtering**

Port Range: -
 Protocol:
 Comment:


Current Filter Table:

Port Range	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

the list, highlight it and click “Delete Selected” (or “Delete All” if you’ve highlighted more than one). To clear all current selections, click “Reset.” To clear all current text fields, click “Cancel.”

3.5.3 IP Filtering

This section allows you to prevent users from accessing certain Internet applications/services (e.g., Web sites, e-mail, FTP sites) by restricting the flow of certain types of data packets. (See Port Filtering above.)


INTELLINET
WIRELESS G BROADBAND ROUTER

[Home](#) | [General Setup](#) | [Status](#) | [Tools](#)

- System
- WAN
- LAN
- Wireless
- Firewall**
 - URL Filtering
 - Port Filtering
 - IP Filtering**
 - MAC Filtering
 - Port Forwarding
 - Special Application
 - DMZ

IP Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ **Enable IP Filtering**

Local IP Address: -
 Protocol:
 Comment:

Current Filter Table:

Local IP Address	Protocol	Comment	Select
<input type="button" value="Delete Selected"/> <input type="button" value="Delete All"/> <input type="button" value="Reset"/>			

Enable IP Filtering: Select to activate the function.

Local IP Address / Protocol / Comment: For any item to which you want to apply the IP filtering rules, enter a local IP address, select one of the protocols from the drop-down menu, add any comments that can help identify the item whenever you refer to the list, then click “Apply.” Once one or more filters are applied, the resulting Current Filter Table list will display at the bottom of the screen. To remove an item from the list, highlight it and click “Delete Selected” (or “Delete All” if you’ve highlighted more than one). To clear all current selections, click “Reset.” To clear all current text fields, click “Cancel.”

3.5.4 MAC Filtering

This section allows you to prevent users from accessing certain Internet applications/services (e.g., Web sites, e-mail, FTP sites) by restricting the flow of certain types of data packets. (See Port / IP Filtering above.)

The screenshot shows the 'MAC Filtering' configuration page of an INTELLINET router. The left sidebar contains a navigation menu with options: System, WAN, LAN, Wireless, Firewall (selected), URL Filtering, Port Filtering, IP Filtering, MAC Filtering (highlighted), Port Forwarding, Special Application, and DMZ. The main content area is titled 'MAC Filtering' and includes a description: 'Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.' Below this is a checkbox for 'Enable MAC Filtering'. There are input fields for 'MAC Address' and 'Comment'. 'Apply' and 'Cancel' buttons are present. A 'Current Filter Table' section contains a table with columns 'MAC Address', 'Comment', and 'Select'. Below the table are buttons for 'Delete Selected', 'Delete All', and 'Reset'.

MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

☐ Enable MAC Filtering

MAC Address: Comment:

Current Filter Table:

MAC Address	Comment	Select
-------------	---------	--------

Enable MAC Filtering: Select to activate the function.

MAC Address / Comment: For any item you want to to which you want to apply the MAC filtering rules, enter a MAC address, add any comments that can help identify the item whenever you refer to the list, then click “Apply.” Once one or more items are listed, the resulting Current Filter Table list will display at the bottom of the screen. To

remove an item from the list, highlight it and click “Delete Selected” (or “Delete All” if you’ve highlighted more than one). To clear all current selections, click “Reset.” To clear all current text fields, click “Cancel.”

3.5.5 Port Forwarding

This section allows you to re-direct a particular range of service port numbers (from the Internet / WAN ports) to a particular LAN IP address. This helps you host some servers behind the router’s NAT firewall.

INTELLINET WIRELESS G BROADBAND ROUTER

Home | General Setup | Status | Tools

- System
- WAN
- LAN
- Wireless
- Firewall**
 - URL Filtering
 - Port Filtering
 - IP Filtering
 - MAC Filtering
 - Port Forwarding
 - Special Application
 - DMZ

Port Forwarding

behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

☐ Enable Port Forwarding

IP Address: Protocol: Port Range: - Comment:

Current Port Forwarding Table:

Local IP Address	Protocol	Port Range	Comment	Select
------------------	----------	------------	---------	--------

Enable Port Forwarding: Select to activate the function.

IP Address: Enter the private IP address of the server behind the NAT firewall. **NOTE:** You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.

Protocol: Select the protocol type to be forwarded: “TCP” or “UDP,” or both.

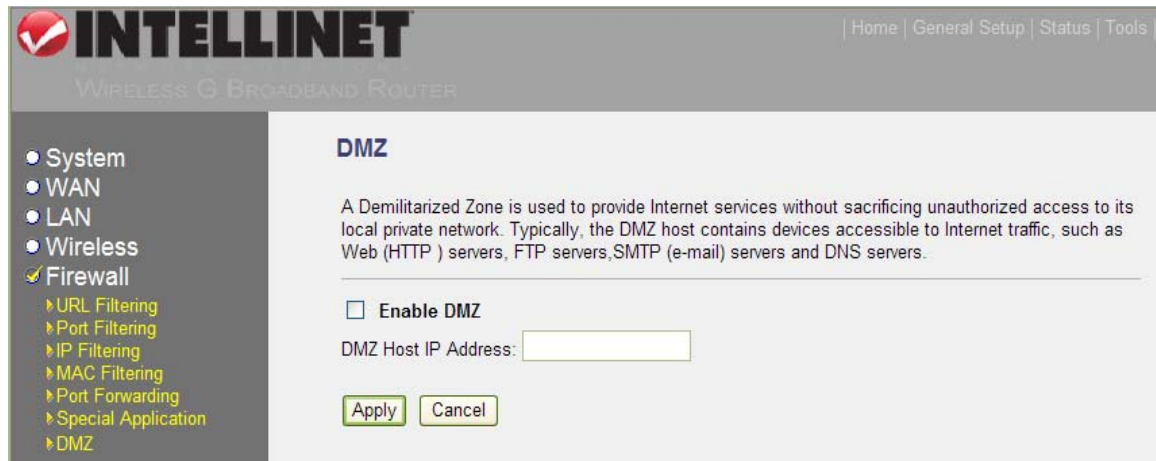
Port Range: Enter the range of ports to be forwarded to the private IP.

Comment: Enter a description of the item being filtered, then click “Apply.”

Once one or more items are listed, the resulting Current Port Forwarding Table list will display at the bottom of the screen. To remove an item from the list, highlight it and click “Delete Selected” (or “Delete All” if you’ve highlighted more than one). To clear all current selections, click “Reset.” To clear all current text fields, click “Cancel.”

3.5.6 DMZ

If you have a local client PC that can't run an Internet application properly from behind the NAT firewall (games, for example), then you can open the client up to unrestricted two-way Internet access by defining a DMZ host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN.



The screenshot shows the web interface of an INTELLINET Wireless G Broadband Router. The top navigation bar includes links for Home, General Setup, Status, and Tools. A left sidebar contains a menu with options: System, WAN, LAN, Wireless, Firewall (selected), URL Filtering, Port Filtering, IP Filtering, MAC Filtering, Port Forwarding, Special Application, and DMZ. The main content area is titled 'DMZ' and contains a description: 'A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.' Below this, there is a checkbox labeled 'Enable DMZ' which is currently unchecked. Underneath the checkbox is a text input field labeled 'DMZ Host IP Address:'. At the bottom of the configuration area are two buttons: 'Apply' and 'Cancel'.

Enable DMZ: Select to activate the function.

DMZ Host IP Address: Enter the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port / public IP address above. **NOTE:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

You can now configure other advanced sections or start using the router with the advanced settings in place.

4 STATUS

The Status section allows you to monitor and reference such things as the connection status of the router's WAN/LAN interfaces, the current firmware version numbers and any illegal attempts to access your network. In addition, it contains the system log and the statistics screen.

The screenshot shows the 'Status Information' page of the INTELLINET Wireless G Broadband Router. The left sidebar contains a 'Status' menu with sub-items 'System Log' and 'Statistics'. The main content area displays the following information:

System	
Uptime	0day:3h:0m:27s
Firmware Version	1.02

Wireless Settings	
Mode	AP
Band	2.4 GHz (B+G)
SSID	INTELLINET
Channel Number	11
Encryption	Disabled
BSSID	00:1f:1f:1f:70:04
Associated Clients	0

TCP/IP Configuration	
Attain IP Protocol	Fixed IP
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DHCP Server	Enabled
MAC Address	00:1f:1f:1f:70:04

WAN Settings	
Attain IP Protocol	DHCP
IP Address	10.10.10.93
Subnet Mask	255.255.252.0
Default Gateway	10.10.8.1

4.1 System Log

This screen displays any event occurring after system startup.

The screenshot shows the 'System Log' page of the INTELLINET Wireless G Broadband Router. The left sidebar contains a 'Status' menu with sub-items 'System Log' and 'Statistics'. The main content area displays the following information:

This page can be used to set remote log server and show the system log.

☐ Enable Log

☒ wireless only ☐ system all

☐ Enable Remote Log

Log Server IP Address:

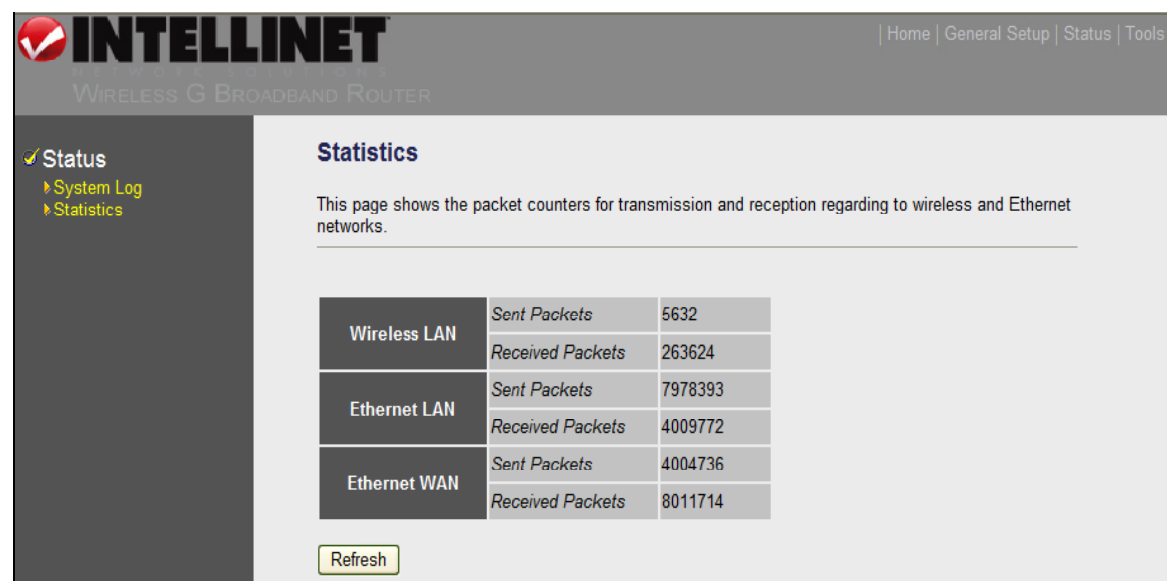
Enable Log: Select to activate the function, then select either “wireless only” or “system all.”

Enable Remote Log / Log Server IP Address: Select to send all log information to a remote server, and enter the server IP address in the text field.

Click “Refresh” to view the most recent informatino; click “Clear” to remove current data. When the system is powered down, the system log will disappear if not saved to a local file.

4.2 Statistics

This screen displays pertinent information about WAN, LAN and WLAN packet transmissions.

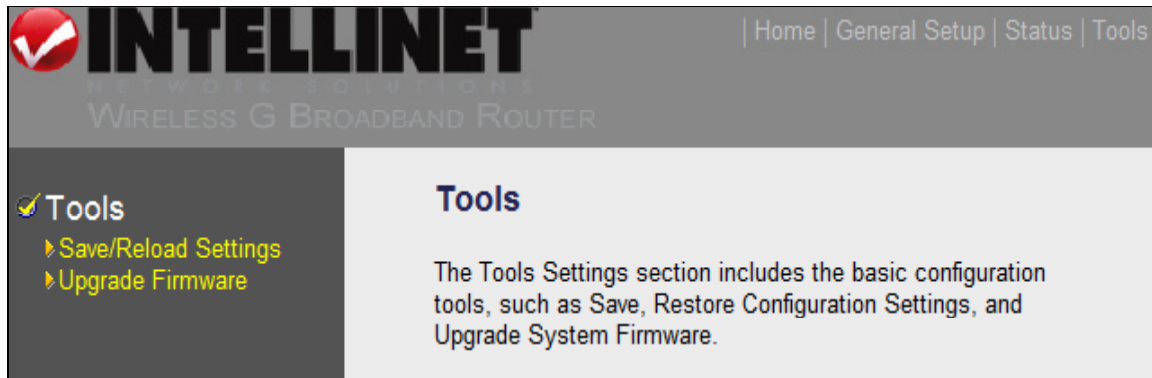


The screenshot shows the 'Statistics' page of an INTELLINET Wireless G Broadband Router. The page has a header with the INTELLINET logo and navigation links: Home, General Setup, Status, and Tools. A left sidebar contains a 'Status' menu with 'System Log' and 'Statistics' options. The main content area is titled 'Statistics' and includes a descriptive text: 'This page shows the packet counters for transmission and reception regarding to wireless and Ethernet networks.' Below this text is a table with packet statistics for three network types: Wireless LAN, Ethernet LAN, and Ethernet WAN. Each network type has two rows: 'Sent Packets' and 'Received Packets'. A 'Refresh' button is located at the bottom of the table.

Network Type	Category	Value
Wireless LAN	Sent Packets	5632
	Received Packets	263624
Ethernet LAN	Sent Packets	7978393
	Received Packets	4009772
Ethernet WAN	Sent Packets	4004736
	Received Packets	8011714

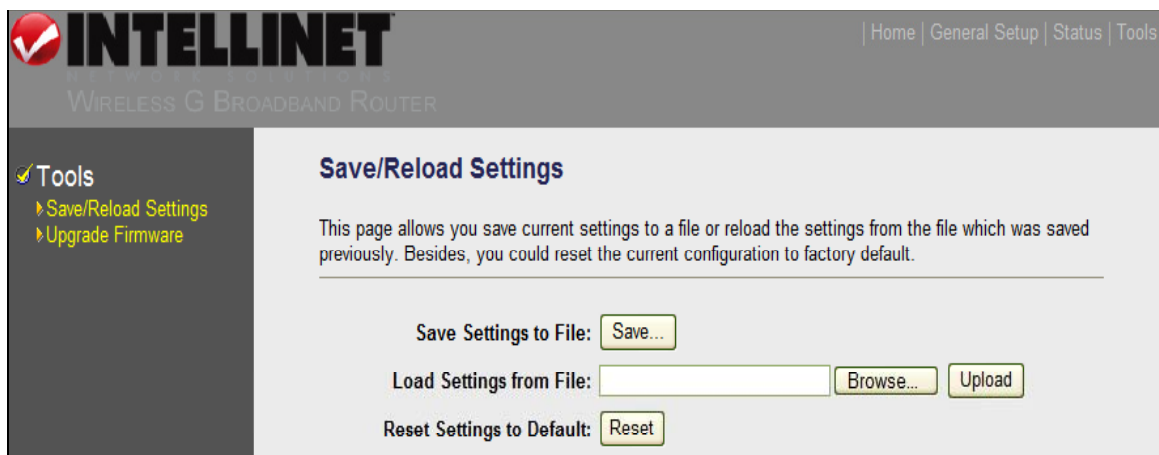
5 TOOLS

This section allows you to save or restore configuration settings and upgrade system firmware.



5.1 Save/Reload Settings

This screen allows you to save (back up) the router's current configuration settings, which, of course, provides added protection and convenience should problems occur with the router and you have to reset to factory defaults.



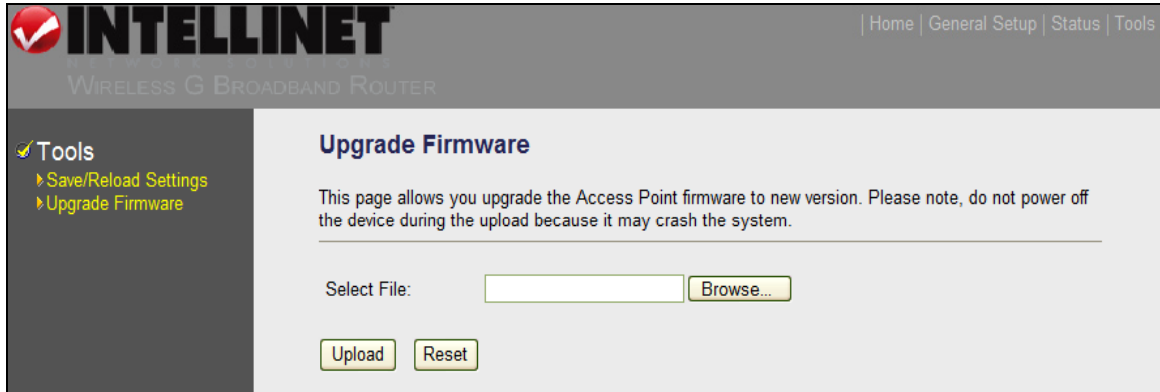
Save Settings to File: Click “Save” to place the current configuration in the “config.bin” file on your PC.

Load Settings from File: Click “Browse” to locate the previously saved configuration file; then click “Upload” to restore the configuration.

Reset Settings to Default: Click “Reset” to force the router to perform a power reset and restore the original factory settings (as they were when you first purchased the router).

5.2 Upgrade Firmware

This screen allows you to upgrade the Wireless G 4-Port Router's system firmware. To do so, you need to download the firmware file to your local hard drive.



The screenshot shows the 'Upgrade Firmware' page of the INTELLINET Wireless G Broadband Router. The page has a dark grey header with the INTELLINET logo and navigation links: Home, General Setup, Status, and Tools. Below the header, there's a sidebar on the left with a 'Tools' menu containing 'Save/Reload Settings' and 'Upgrade Firmware'. The main content area is titled 'Upgrade Firmware' and contains a warning: 'This page allows you upgrade the Access Point firmware to new version. Please note, do not power off the device during the upload because it may crash the system.' Below this, there is a 'Select File:' label, a text input field, and a 'Browse...' button. At the bottom of the main area, there are 'Upload' and 'Reset' buttons.

Select File: Enter the filename of the firmware already downloaded to the hard drive field, or click “Browse” to locate the file. Click “Upgrade” to begin the firmware upgrade (which may take a few minutes).

NOTE: Be careful that you don't turn off the router during the firmware upload, as this can crash the system. Once the upgrade is complete, you can start using the router again.

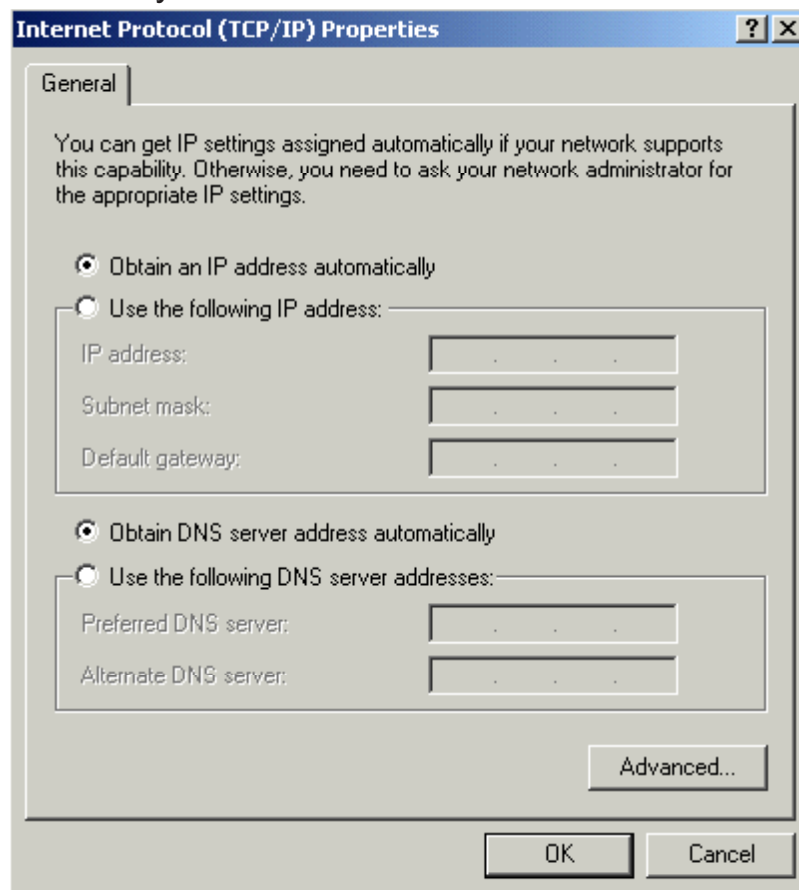
APPENDIX A

This section presents the basic steps for using Windows 2000, XP or Vista to obtain an IP address automatically, as directed in the Quick Installation section.

Windows 2000

1. Go to Start → Settings → Control Panel.
2. Double-click on the Network and Dial-up Connections icon. In the Network and Dial-up Connection window, double-click on the Local Area Connection icon.
3. In the Local Area Connection window, click “Properties.”
4. Check your list of Network Components. You should see “Internet Protocol [TCP/IP]” on your list. Select it and click “Properties.”
5. In the Internet Protocol (TCP/IP) Properties window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
6. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically from your router’s DHCP server.

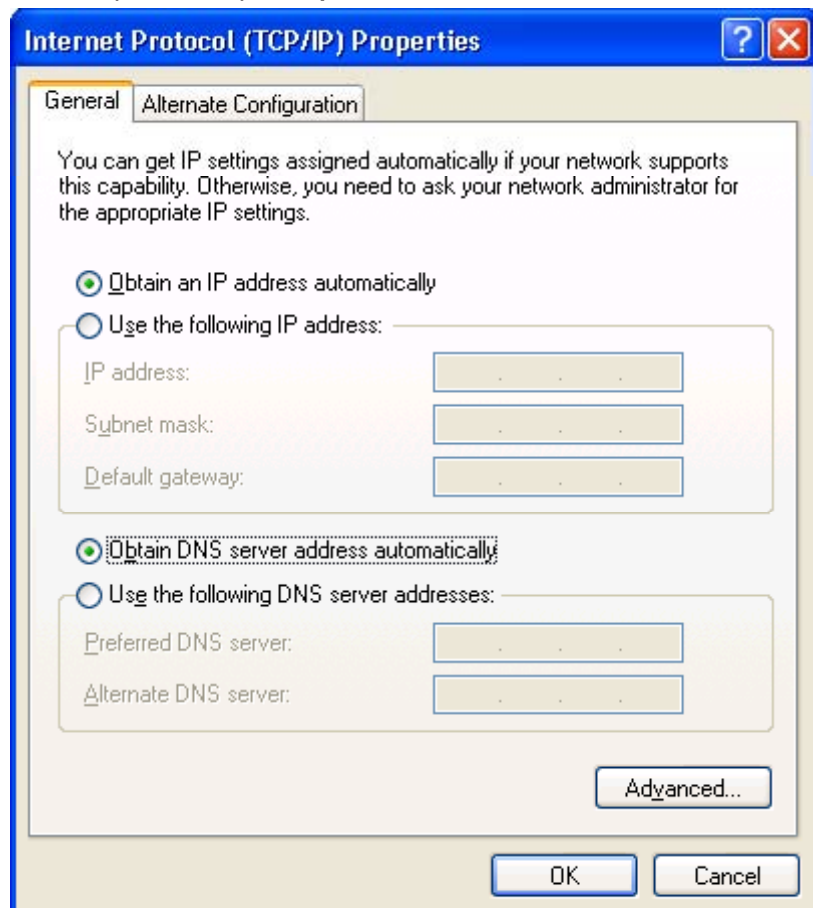
NOTE: Make sure that the Wireless G 4-Port Router’s DHCP server is the only DHCP server available on your LAN.



Windows XP

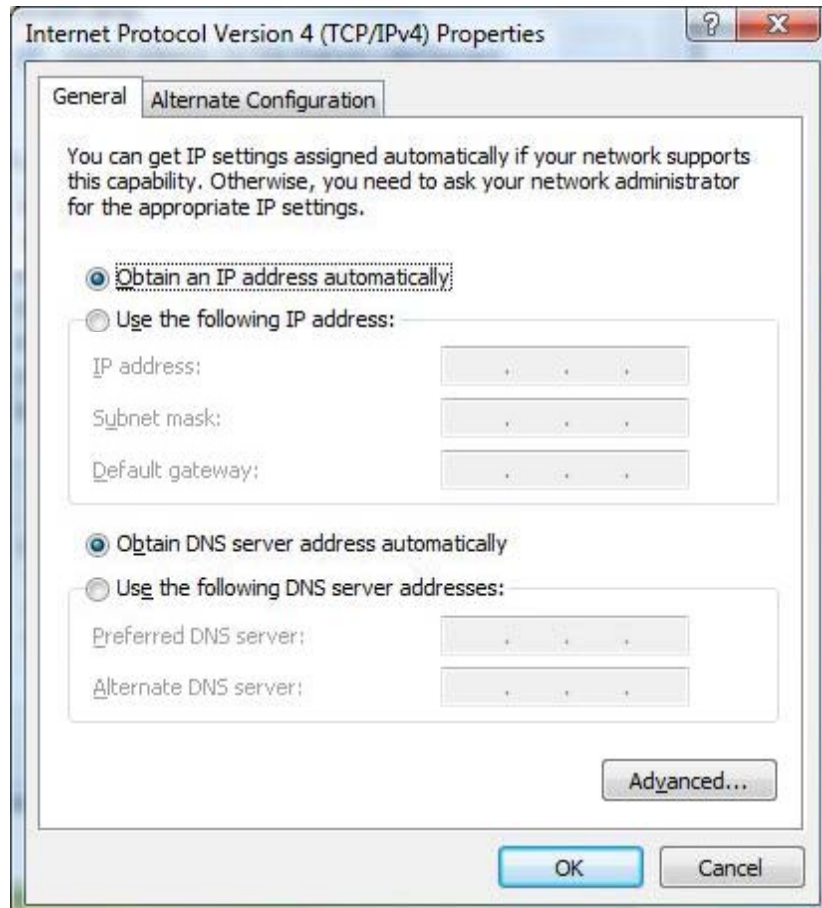
1. Go to Start → Settings, then click “Network Connections.”
2. Double-click on the Local Area Connection icon.
3. Check your list of Network Components. You should see “Internet Protocol [TCP/IP]” on your list. Select it and click “Properties.”
4. In the Internet Protocol (TCP/IP) Properties window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
5. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically from your router’s DHCP server.

NOTE: Make sure that the Wireless G 4-Port Router’s DHCP server is the only DHCP server available on your LAN.



Windows Vista

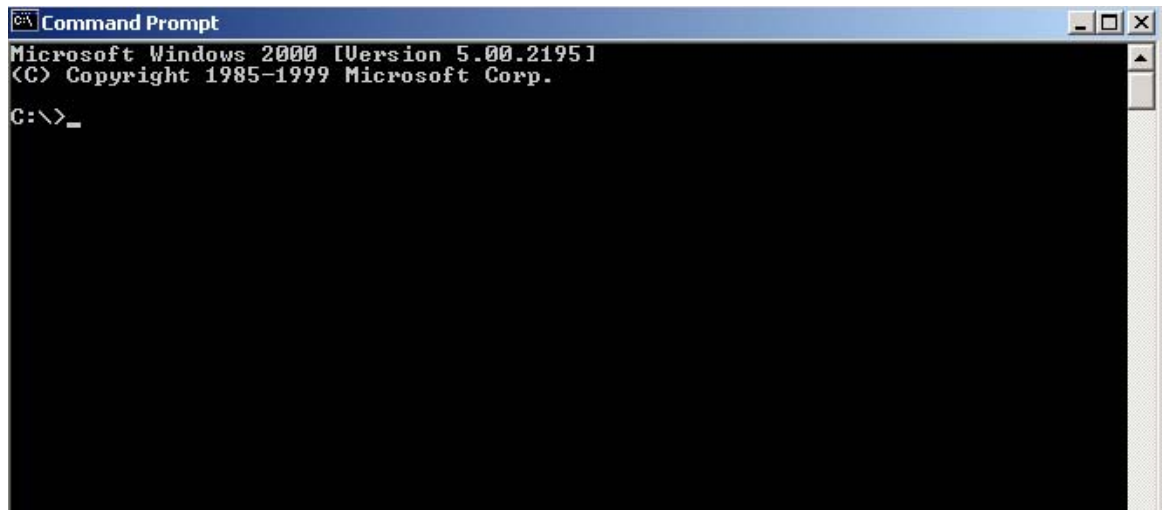
1. Go to Start → Settings → Control Panel.
2. Double-click Network and Sharing Center.
3. Click “Manage network connections”; right-click on the Local Area Connection icon; then select “Properties.”
4. Check your list of Network Components. You should see “Internet Protocol Version 4 (TCP/IPv4)” on your list. Select it and click “Properties.”
5. In the Internet Protocol Version 4 (TCP/IPv4) Properties window, select “Obtain an IP address automatically” and “Obtain DNS server address automatically.”
6. Click “OK” to confirm the setting. Your PC will now obtain an IP address automatically from your router’s DHCP server.



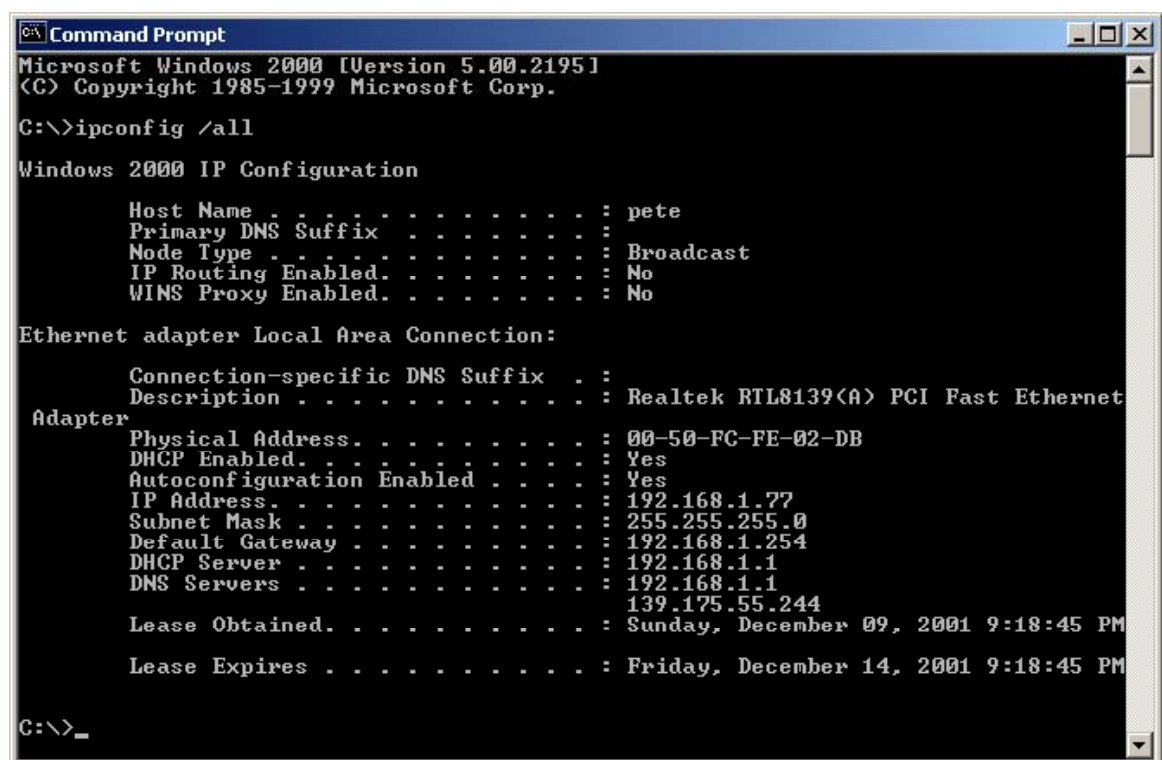
NOTE: Make sure that the Wireless G 4-Port Router’s DHCP server is the only DHCP server available on your LAN.

APPENDIX B

To manually find your PC's IP and MAC addresses in Windows, open the Command Prompt program, type "Ipconfig /all" and press the Enter key.



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>_
```



```
Command Prompt
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.
C:\>ipconfig /all

Windows 2000 IP Configuration

    Host Name . . . . . : pete
    Primary DNS Suffix . . . . . :
    Node Type . . . . . : Broadcast
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Description . . . . . : Realtek RTL8139(A) PCI Fast Ethernet
    Adapter
    Physical Address. . . . . : 00-50-FC-FE-02-DB
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.77
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.1
                           139.175.55.244
    Lease Obtained. . . . . : Sunday, December 09, 2001 9:18:45 PM
    Lease Expires . . . . . : Friday, December 14, 2001 9:18:45 PM

C:\>_
```

Your PC's IP address is listed as "IP address (192.168.1.77)."
The router's IP address is listed as "Default Gateway (192.168.1.254)."
Your PC's MAC address is listed as "Physical Address (00-50-FC-FE-02-DB)."

GLOSSARY

Default Gateway: Every non-router IP device needs to configure a default gateway's IP address. When the device sends out an IP packet, if the destination is not on the same network the device has to send the packet to its default gateway, which will then send it out toward the destination.

DHCP: The Dynamic Host Configuration Protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: The Domain Name System allows Internet servers to have a domain name (such as www.Broadbandrouter.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as when typing "Broadbandrouter.com" into your Internet browser) the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: A Digital Subscriber Line modem uses existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

Idle Timeout: Idle Timeout is designed so that after there is no traffic to the Internet for a pre-configured amount of time, the connection will automatically be disconnected.

IP Address and Network (Subnet) Mask: An Internet Protocol address consists of a series of four numbers — separated by periods — that identifies a single, unique Internet computer host in an IP network. As an example, 192.168.2.1 consists of two sections: the IP network address and the host identifier. The IP address is a 32-bit binary pattern that can be represented as four cascaded decimal numbers separated by periods: `aaa.aaa.aaa.aaa`, where each "aaa" can be anything from 000 to 255; or as four cascaded binary numbers separated by periods: `bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb`, where each "b" can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of

consecutive leading 1's followed by consecutive trailing 0's, such as 11111111.11111111.11111111.00000000. Therefore, a network mask can sometimes be described simply as "x" number of leading 1's.

When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1's in the network mask become part of the IP network address, and the remaining bits correspond to the host ID. For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is 11111111.11111111.11110000.00000000, then its network address is 11011001.10110000.10010000.00000000 and its host ID is 00000000.00000000.00000000.00000111. This is a convenient and efficient method for routers to route IP packets to their destination.

ISP Gateway Address: This is an IP address for the Internet router located at the ISP's office.

ISP: An Internet Service Provider is a business that provides connectivity to the Internet for individuals, businesses or organizations.

LAN: A Local Area Network is a group of computers and devices connected together in a relatively small area, such as a house or office. Your home network is considered a LAN.

MAC Address: A Media Access Control address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It's composed of two parts: 3 bytes of data corresponding to the manufacturer ID (unique for each manufacturer), plus 3 bytes often used as the product's serial number.

NAT: Network Address Translation is a process that allows all of the computers on your home network to use one IP address. Using the router's NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.

Port: Network clients (LAN PC) uses port numbers to distinguish one network application/protocol from another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

PPPoE: Point-to-Point Protocol over Ethernet, a communications protocol for transmitting data over the Ethernet among different manufacturers, is a secure data transmission method originally created for dial-up connections (PPPoE is for Ethernet connections). PPPoE relies on two widely accepted standards: Ethernet and the Point-to-Point Protocol.

Protocol: A protocol is a set of rules for interaction agreed upon by multiple parties so that when they interface with each other based on such a protocol, the interpretation of their behavior is well defined and can be made objectively, without confusion or misunderstanding.

Router: A router is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g., 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol and Unreliable Datagram Protocol. TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocols. TCP performs proper error detection and error recovery, and thus is reliable. UDP, on the other hand, is not reliable. Both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: A Wide Area Network connects computers in separate areas (e.g., different buildings, cities, countries). The Internet is a WAN.

Web-based Management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the Web browser. This means the user can use the familiar Netscape or MS Internet Explorer to control or monitor the device being managed.

SPECIFICATIONS

Standards

- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.1x (Wireless User Authentication)
- IEEE 802.11b (11 Mbps Wireless LAN)
- IEEE 802.11g (54 Mbps Wireless LAN)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3u (100Base-TX Fast Ethernet)

General

- LAN ports: 4 RJ45 10/100 Mbps data ports
- LAN ports with Auto MDI/MDI-X
- Certifications: FCC Class B, CE Mark, RoHS

Router

- Chipset: Realtek RTL8186
- Supported WAN connection types:
 - Dynamic IP (DHCP for cable service)
 - Static IP
 - PPPoE (for DSL)
- Protocols:
 - CSMA/CA
 - CSMA/CD
 - TCP/IP
 - UDP
 - ICMP
 - PPPoE
 - NTP
 - NAT (network address

translation)

- DHCP
- DNS
- NAT:
 - Port forwarding
- Firewall:
 - Port filter
 - IP filter
 - Access control based on MAC address
 - DMZ (demilitarized zone)
- Supports UPNP (Universal Plug and Play)
- Supports DHCP (client/server)
- Supports PPPoE (DSL), DHCP (cable) and static IP
- Supports VPN PPTP, L2TP and IPsec pass-through

Wireless

- Chipset: RTL8225
- Wireless frequency range: 2.412 - 2.484 GHz
- Modulation technologies:
 - 802.11b: Direct Sequence Spread Spectrum (DSSS): DBPSK, DQPSK, CCK
 - 802.11g: Orthogonal Frequency Division Multiplexing (OFDM): BPSK, QPSK, 16QAM, 64QAM
- Number of channels: 11
- Data rates:
 - IEEE 802.11b (11 Mbps, 5.5 Mbps, 2 Mbps, 1 Mbps)
 - IEEE 802.11g (54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18

- Mbps, 12 Mbps, 9 Mbps, 6 Mbps)
- Output power:
 - OFDM: 15 dBm +/- 1 dBm (54 Mbps, 50 mW max.)
 - CCK: 17 dBm +/- 1 dBm (11 Mbps, 50 mW max.)
- Maximum coverage distance:
 - 100 m / 300 ft. (indoor),
 - 300 m / 900 ft. (outdoor)
- Wireless security:
 - WEP encryption (64-/128-bit)
 - WPA (TKIP and AES)
 - WPA2 (TKIP and AES)
 - Client access control through media access control (MAC) filter
- Antenna: single dipole antenna, 2 dBi gain

LEDs

- Power
- WLAN Link/Act
- WAN Link/Act
- LAN 1-4 Link/Act

Environmental

- Dimensions: 157 (W) x 127 (L) x 30 (H) mm (6.2 x 5.0 x 1.2 in.)
- Weight: 0.8 kg (1.7 lbs.)
- Operating temperature: 0 – 40°C (32 – 104°F)
- Operating humidity: 10 – 90% RH, non-condensing
- Storage temperature: -20 – 60°C (4 – 149°F)

Power

- External power adapter: 12 V DC, 1.0 A
- Power consumption: 5.5 Watts max.

Package Contents

- Wireless G 4-Port Router
- User manual
- Power adapter
- Ethernet Cat5 RJ45 cable, 1.0 m (3 ft.)



INTELLINETTM

N E T W O R K S O L U T I O N S

INTELLINET NETWORK SOLUTIONSTM offers a complete line
of active and passive networking products.

Ask your local computer dealer for more information or visit

www.intellinet-network.com.

Copyright © INTELLINET NETWORK SOLUTIONS

All products mentioned are trademarks or registered trademarks of their respective owners.